kaspersky

Kaspersky Security Center 14.2 Windows

Spis treści

System pomocy Kaspersky Security Center 14.2

Nowości Zapoznaj się z nowościami w najnowszym wydaniu produktu.	**Konfigurowanie ochrony sieci** Zarządzaj bezpieczeństwem organizacji.
Wymagania sprzętowe i programowe Sprawdź, które systemy operacyjne i wersje aplikacji są obsługiwane.	**Aplikacje Kaspersky. Aktualizowanie baz danych i modułów aplikacji** Zachowaj niezawodność systemu ochrony.
Instalacja i wstępna konfiguracja Rozplanuj korzystanie z zasobów, instalację Serwera administracyjnego, instalację Agenta sieciowego i aplikacji zabezpieczających na urządzeniach klienckich, a także przyłączenie urządzeń do grup administracyjnych.	**Monitorowanie i raportowanie** Sprawdź swoją infrastrukturę, stany ochrony i statystyki.
Wykrywanie urządzeń w sieci Wyszukuj istniejące i nowe urządzenia w sieci organizacji.	**Zastępowanie aplikacji zabezpieczających firm trzecich** Poznaj metody odinstalowywania niekompatybilnych aplikacji.
Aplikacje Kaspersky. Zdalna instalacja Zdalnie instaluj aplikacje Kaspersky.	**Dostosowanie punktów dystrybucji i bram połączenia** Konfiguruj punkty dystrybucji.
Aktualizowanie Kaspersky Security Center z poprzedniej wersji Aktualizuj Kaspersky Security Center 14.2 z poprzedniej wersji.	**Praktyczne zastosowanie aplikacji dla dostawców usługi (tylko pomoc online)** Zapoznaj się z zaleceniami dotyczącymi instalacji, konfiguracji i korzystania z aplikacji, a także sposobami rozwiązywania typowych problemów występujących podczas działania aplikacji.
Aplikacje Kaspersky. Licencjonowanie i aktywacja Aktywuj aplikacje Kaspersky w kilku krokach.	**Podręcznik szacowania rozmiaru (tylko pomoc online)** Aby zapewnić optymalną wydajność w różnych warunkach pracy, należy wziąć pod uwagę liczbę urządzeń w sieci, topologię sieci oraz zestaw funkcji Kaspersky Security Center, jakich potrzebujesz.
Eksportowanie zdarzeń do systemów SIEM Skonfiguruj eksportowanie zdarzeń do systemów SIEM w celu przeprowadzenia analizy.	**Zarządzanie lukami i poprawkami** Wyszukaj i wyeliminuj luki w oprogramowaniu firm trzecich.
Praca w środowisku chmury Zainstaluj Kaspersky Security Center w środowiskach chmury: Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.	**Często Zadawane Pytania (Tylko angielski)** Znajdź instrukcje rozwiązywania typowych problemów.

	Przewodnik szybkiego uruchomienia Kaspersky Endpoint Security for Business Zacznij korzystać z Kaspersky Endpoint Security for Business: zainstaluj i skonfiguruj to rozwiązanie. Możesz również sprawdzić porównanie funkcji Kaspersky Security Center, aby wybrać najbardziej odpowiedni sposób zarządzania bezpieczeństwem sieci.		

Nowości

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 posiada kilka nowych funkcji i ulepszeń:

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

  Zainstaluj również najnowszą aktualizację Kaspersky Security Center. Ta aktualizacja zawiera funkcje ochrony infrastruktury, takie jak dwuetapowa weryfikacja kont użytkowników i inne ulepszenia.

- Dostęp do serwerów Kaspersky jest teraz weryfikowany automatycznie. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznego DNS.

- Uprawnienia użytkownika na wirtualnym Serwerze administracyjnym są dostępne do konfiguracji w dowolnym momencie niezależnie od podstawowego Serwera administracyjnego. Użytkownikom Serwera podstawowego można również przypisać prawa do zarządzania Serwerem wirtualnym.

- Kaspersky Security Center obsługuje teraz pracę z następującymi systemami DBMS:

  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro Standard 13.x
  - Postgres Pro Standard 14.x
  - Postgres Pro Certified 14.x
  - MariaDB 10.1, 10.4, 10.5

- Możesz użyć Kaspersky Security Center Web Console do wyeksportowania zasad i zadań do pliku, a następnie zaimportowania zasad i zadań do Kaspersky Security Center Windows lub Kaspersky Security Center Linux.

- Opcja **Nie używaj serwera proxy** została usunięta z następujących zadań:

  - *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
  - *Pobierz aktualizacje do repozytoriów punktów dystrybucji*

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

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

Kaspersky Security Center 14

Kaspersky Security Center 14 posiada kilka nowych funkcji i ulepszeń:

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

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

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

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

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

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

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

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

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

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

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 posiada kilka nowych funkcji i ulepszeń:

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

- Kaspersky Security Center pracuje teraz z adresami IPv6 oraz z adresami IPv4. Serwer administracyjny może przeszukiwać sieci posiadające urządzenia z adresami IPv6.

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

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

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 posiada kilka nowych funkcji i ulepszeń:

- Udoskonalono integrację z systemami SIEM. Teraz można wyeksportować zdarzenia do systemów SIEM za pośrednictwem zaszyfrowanego kanału (TLS). Funkcja jest dostępna w przypadku Kaspersky Security Center Web Console i Konsoli administracyjnej opartej na MMC.
- Teraz możesz pobierać poprawki dla Serwera administracyjnego jako pakiet dystrybucyjny, którego możesz używać do przyszłych aktualizacji do nowszych wersji.
- Do Kaspersky Security Center 13.1 Web Console, dla Kaspersky Endpoint Detection and Response Optimum dodano nową sekcję **Powiadomienia**. Do pracy z zagrożeniami wykrytymi przez Kaspersky Endpoint Detection and Response Optimum dodano kilka nowych widżetów.
- W Kaspersky Security Center 13.1 Web Console możesz teraz otrzymywać powiadomienia na temat wygasłych licencji dla aplikacji firmy Kaspersky.
- Czas odpowiedzi dla Kaspersky Security Center 13.1 Web Console został wydłużony.

Kaspersky Security Center 13

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

- Zaimplementowano weryfikację dwuetapową. Możesz włączyć weryfikację dwuetapową, aby zmniejszyć ryzyko nieautoryzowanego dostępu do konsoli Kaspersky Security Center 13 Web Console.
- Zaimplementowano uwierzytelnianie domeny przy użyciu protokołów NTLM i Kerberos (technologia pojedynczego logowania). Funkcja pojedynczego logowania umożliwia użytkownikowi systemu Windows włączenie bezpiecznego uwierzytelniania w konsoli Kaspersky Security Center 13 Web Console bez konieczności ponownego wprowadzania hasła w sieci firmowej.
- Teraz możesz skonfigurować wtyczkę do pracy z Kaspersky Managed Detection and Response. Możesz użyć tej integracji do przeglądania incydentów i zarządzania stacjami roboczymi.

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

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

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

- Możesz teraz otworzyć dowolny raport, klikając jego nazwę.

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

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

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

Do Kaspersky Security Center 13 dodano następujące funkcje:

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

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

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

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

Kaspersky Security Center 14.2

Ta sekcja zawiera informacje na temat korzystania z Kaspersky Security Center 14.2.

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

Informacje o Kaspersky Security Center

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

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

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

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

Korzystając z Kaspersky Security Center, możesz:

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

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

- Utworzyć hierarchię grup administracyjnych, aby zarządzać wyborem urządzeń klienckich jako całością.

- Zarządzać systemem ochrony antywirusowej zbudowanym w oparciu o aplikacje Kaspersky.

- Utworzyć obrazy systemów operacyjnych i instalować je na urządzeniach klienckich w sieci oraz wykonywać zdalną instalację aplikacji firmy Kaspersky i innych dostawców oprogramowania.

- Zdalnie zarządzać aplikacjami firmy Kaspersky i innych producentów, które są zainstalowane na urządzeniach klienckich. Instalować aktualizacje, wyszukiwać i eliminować luki.

- Wykonywać scentralizowane rozsyłanie kluczy licencyjnych dla aplikacji Kaspersky na urządzenia klienckie, monitorowanie ich wykorzystania i odnawianie licencji.

- Otrzymywać statystyki i raporty dotyczące pracy aplikacji i urządzeń.

- Otrzymywać powiadomienia na temat zdarzeń krytycznych występujących podczas działania aplikacji Kaspersky.
- Zarządzać urządzeniami mobilnymi.
- Zarządzać szyfrowaniem informacji przechowywanych na dyskach twardych urządzeń i nośników wymiennych oraz dostępem użytkowników do zaszyfrowanych danych.
- Wykonywać inwentaryzację sprzętu podłączonego do sieci firmy.
- Centralnie zarządzać plikami umieszczonymi w Kwarantannie lub Kopii zapasowej przez aplikacje zabezpieczające, a także zarządzać plikami, których przetwarzanie zostało odroczone.

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

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

Wymagania sprzętowe i programowe

Serwer administracyjny

Minimalne wymagania sprzętowe:

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

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

Wymagania programowe:

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

Obsługiwane są następujące systemy operacyjne:

- Windows Server 2008 R2 Standard z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 z pakietem Service Pack 1 (wszystkie wersje) 64-bitowy
- Windows Server 2012 Server Core 64-bitowy

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

Obsługiwane są następujące platformy wirtualizacji:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64-bitowy
- Microsoft Hyper-V Server 2012 R2 64-bitowy

- Microsoft Hyper-V Server 2016 64-bitowy
- Microsoft Hyper-V Server 2019 64-bitowy
- Microsoft Hyper-V Server 2022 64-bitowy
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x (tylko podczas logowania jako gość systemu Windows)

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

- Microsoft SQL Server 2012 Express 64-bitowy
- Microsoft SQL Server 2014 Express 64-bitowy
- Microsoft SQL Server 2016 Express 64-bitowy
- Microsoft SQL Server 2017 Express 64-bitowy
- Microsoft SQL Server 2019 Express 64-bitowy
- Microsoft SQL Server 2014 (wszystkie wersje) 64-bitowy
- Microsoft SQL Server 2016 (wszystkie wersje) 64-bitowy
- Microsoft SQL Server 2017 (wszystkie wersje) na 64-bitowy system Windows
- Microsoft SQL Server 2017 (wszystkie wersje) na 64-bitowy system Linux
- Microsoft SQL Server 2019 (wszystkie edycje) na 64-bitowy system Windows (wymaga dodatkowych działań)
- Microsoft SQL Server 2019 (wszystkie edycje) na 64-bitowy system Linux (wymaga dodatkowych działań)
- Baza danych Microsoft Azure SQL
- Wszystkie obsługiwane wersje serwera SQL w platformach chmury Amazon RDS i Microsoft Azure
- MySQL 5.7 Community 32-bitowy/64-bitowy
- MySQL Standard Edition 8.0 (wersja 8.0.20 i nowsze) 32-bitowy/64-bitowy
- MySQL Enterprise Edition 8.0 (wersja 8.0.20 i nowsze) 32-bitowy/64-bitowy
- MariaDB 10.1 (kompilacja 10.1.30 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.3 (kompilacja 10.3.22 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.4 (kompilacja 10.4.26 i nowsze) 32-bitowe/64-bitowe
- MariaDB 10.5 (kompilacja 10.5.17 i nowsze) 32-bitowe/64-bitowe

- MariaDB Server 10.3 32-bitowy/64-bitowy z silnikiem magazynowania InnoDB
- MariaDB Galera Cluster 10.3 32-bitowy/64-bitowy z silnikiem magazynowania InnoDB
- PostgreSQL 13.x 64-bitowy
- PostgreSQL 14.x 64-bitowy
- Postgres Pro Standard 13.x 64-bitowy
- Postgres Pro Standard 14.x 64-bitowy
- Postgres Pro Certified 14.x 64-bitowy

Zalecane jest korzystanie z serwera MariaDB 10.3.22; jeśli używasz wcześniejszej wersji, wykonanie zadania Wykonaj synchronizację Windows Update może zająć dłużej niż jeden dzień.

SIEM i inne systemy zarządzania informacjami:

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

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console Server

Minimalne wymagania sprzętowe:

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

Obsługiwane są następujące systemy operacyjne:

- Microsoft Windows (tylko 64-bitowe wersje):
  - Windows Server 2012 Server Core
  - Windows Server 2012 Datacenter
  - Windows Server 2012 Essentials
  - Windows Server 2012 Foundation
  - Windows Server 2012 Standard
  - Windows Server 2012 R2 Server Core

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

- Linux (tylko wersje 64-bitowe):
  - Debian GNU/Linux 9.x (Stretch)
  - Debian GNU/Linux 10.x (Buster)
  - Debian GNU/Linux 11.x (Bullseye)
  - Ubuntu Server 18.04 LTS (Bionic Beaver)
  - Ubuntu Server 20.04 LTS (Focal Fossa)
  - Ubuntu Server 22.04 LTS (Jammy Jellyfish)
  - CentOS 7.x
  - Red Hat Enterprise Linux Server 7.x
  - Red Hat Enterprise Linux Server 8.x
  - Red Hat Enterprise Linux Server 9.x

- SUSE Linux Enterprise Server 12 (wszystkie pakiety Service Pack)
- SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack)
- Astra Linux Special Edition 1.6 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy)
- Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7.2 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy)
- Astra Linux Common Edition 2.12
- Alt Server 9.2
- Alt Server 10
- Alt 8 SP Server (LKNV.11100-01)
- Alt 8 SP Server (LKNV.11100-02)
- Alt 8 SP Server (LKNV.11100-03)
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition

Maszyna wirtualna oparta na jądrze jest obsługiwana w przypadku następujących systemów operacyjnych zalecanych do wirtualizacji Kaspersky Security Center:

- Alt 8 SP Server (LKNV.11100-01) 64-bitowy
- Alt Server 10 64-bitowy
- Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7.2 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy)
- Debian GNU/Linux 11.x (Bullseye) 32-bitowy/64-bitowy
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-bitowy
- RED OS 7.3 Server 64-bitowy
- RED OS 7.3 Certified Edition 64-bitowy

Urządzenia klienckie

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

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

Przeglądarki:

- Mozilla Firefox Extended Support Release w wersji 91.8.0 lub nowszej (91.8.0 wydano 5 kwietnia 2022 r.)
- Google Chrome w wersji 100.0.4896.88 lub nowszej (wersja oficjalna)
- Microsoft Edge w wersji 100 lub nowszej
- Safari 15 dla systemu macOS

Serwer urządzeń mobilnych iOS MDM

Wymagania sprzętowe:

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

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

Serwer urządzeń mobilnych Exchange

Wszystkie wymagania programowe i sprzętowe serwera urządzeń mobilnych Exchange są zawarte w wymaganiach dla Microsoft Exchange Server.

Obsługiwana jest kompatybilność z Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 i Microsoft Exchange Server 2013.

Konsola administracyjna

Wymagania sprzętowe:

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

Wymagania programowe:

- System operacyjny Microsoft Windows (obsługiwana wersja systemu operacyjnego jest określana przez wymagania Serwera administracyjnego), z wyjątkiem następujących systemów operacyjnych:
  - Windows Server 2012 Server Core 64-bitowy

    - Windows Server 2012 R2 Server Core 64-bitowy
    - Windows Server 2016 Server Core (Opcja instalacji) (LTSB) 64-bitowy
    - Windows Server 2019 Core 64-bitowy
    - Windows Server 2022 Core 64-bitowy
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 10.0 działająca na systemach:
    - Microsoft Windows Server 2008 R2 z Service Pack 1
    - Microsoft Windows Server 2012
    - Microsoft Windows Server 2012 R2
    - Microsoft Windows 7 z Service Pack 1
    - Microsoft Windows 8
    - Microsoft Windows 8.1
    - Microsoft Windows 10
- Microsoft Internet Explorer 11.0 działająca na systemach:
    - Microsoft Windows Server 2012 R2
    - Microsoft Windows Server 2012 R2 z Service Pack 1
    - Microsoft Windows Server 2016
    - Microsoft Windows Server 2019
    - Microsoft Windows 7 z Service Pack 1
    - Microsoft Windows 8.1
    - Microsoft Windows 10
- Microsoft Edge działający pod systemem Microsoft Windows 10

Agent sieciowy

Minimalne wymagania sprzętowe:

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

- Dostępne miejsce na dysku: 1 GB.

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

Obsługiwane są następujące systemy operacyjne:

- Microsoft Windows Embedded POSReady 2009 z najnowszym pakietem Service Pack 32-bitowy
- Microsoft Windows Embedded POSReady 7 32-/64-bitowy
- Microsoft Windows Embedded Standard 7 z dodatkiem Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Standard 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Pro 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Update 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 2015 LTSB 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 2016 LTSB 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-bitowy/ARM
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-bitowy/ARM
- Microsoft Windows 10 Enterprise 2019 LTSC 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1703 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1709 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1803 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1809 32-bitowy/64-bitowy
- Microsoft Windows 10 20H2 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 21H2 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1909 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1607 32-bitowy/64-bitowy
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy

- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS5 (październik 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-bitowy/64-bitowy

- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 11 Home 64-bitowy
- Microsoft Windows 11 Pro 64-bitowy
- Microsoft Windows 11 Enterprise 64-bitowy
- Microsoft Windows 11 Education 64-bitowy
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Pro 32-bitowy/64-bitowy
- Microsoft Windows 8.1 Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 8 Pro 32-bitowy/64-bitowy
- Microsoft Windows 8 Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Home Basic/Premium z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows XP Professional z Service Pack 2 32-bit/64-bit (obsługiwany tylko przez Agenta sieciowego w wersji 10.5)
- Microsoft Windows XP Professional z Service Pack 3 i nowszy, 32-bitowy
- Microsoft Windows XP Professional for Embedded Systems z Service Pack 3 32-bitowy
- Windows Small Business Server 2011 Essentials 64-bitowy
- Windows Small Business Server 2011 Premium Add-on 64-bitowy
- Windows Small Business Server 2011 Standard 64-bitowy

- Windows MultiPoint Server 2011 Standard/Premium 64-bitowy
- Windows MultiPoint Server 2012 Standard/Premium 64-bitowy
- Windows Server 2008 Foundation z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 z dodatkiem Service Pack 2 (wszystkie wersje) 32-bitowy/64-bitowy
- Windows Server 2008 R2 Datacenter z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Enterprise z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Foundation z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Core Mode z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Standard z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 z pakietem Service Pack 1 (wszystkie wersje) 64-bitowy
- Windows Server 2012 Server Core 64-bitowy
- Windows Server 2012 Datacenter 64-bitowy
- Windows Server 2012 Essentials 64-bitowy
- Windows Server 2012 Foundation 64-bitowy
- Windows Server 2012 Standard 64-bitowy
- Windows Server 2012 R2 Server Core 64-bitowy
- Windows Server 2012 R2 Datacenter 64-bitowy
- Windows Server 2012 R2 Essentials 64-bitowy
- Windows Server 2012 R2 Foundation 64-bitowy
- Windows Server 2012 R2 Standard 64-bitowy
- Windows Server 2016 Datacenter (LTSB) 64-bitowy
- Windows Server 2016 Standard (LTSB) 64-bitowy
- Windows Server 2016 Server Core (Opcja instalacji) (LTSB) 64-bitowy
- Windows Server 2019 Standard 64-bitowy
- Windows Server 2019 Datacenter 64-bitowy
- Windows Server 2019 Core 64-bitowy
- Windows Server 2022 Standard 64-bitowy
- Windows Server 2022 Datacenter 64-bitowy

- Windows Server 2022 Core 64-bitowy
- Windows Storage Server 2012 64-bitowy
- Windows Storage Server 2012 R2 64-bitowy
- Windows Storage Server 2016 64-bitowy
- Windows Storage Server 2019 64-bitowy
- Debian GNU/Linux 9.x (Stretch) 32-bitowy/64-bitowy
- Debian GNU/Linux 10.x (Buster) 32-bitowy/64-bitowy
- Debian GNU/Linux 11.x (Bullseye) 32-bitowy/64-bitowy
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-bitowy/64-bitowy
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-bitowy/64-bitowy
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-bitowy
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bitowy/64-bitowy
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bitowy/64-bitowy
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-bitowy
- CentOS 7.x 64-bitowy
- CentOS 7.x ARM 64-bitowy
- Red Hat Enterprise Linux Server 6.x 32-bitowy/64-bitowy
- Red Hat Enterprise Linux Server 7.x 64-bitowy
- Red Hat Enterprise Linux Server 8.x 64-bitowy
- Red Hat Enterprise Linux Server 9.x 64-bitowy
- SUSE Linux Enterprise Server 12 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Desktop 15 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Desktop 15 z Service Pack 3 ARM 64-bitowy
- openSUSE 15 64-bitowy
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64-bitowy
- Astra Linux Common Edition 2.12 64-bitowy

- Astra Linux Special Edition, wersja 1.6 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy) 64-bitowy
- Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7.2 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy) 64-bitowy
- Astra Linux Special Edition 4.7 ARM
- Alt Server 9.2 64-bitowy
- Alt Server 10 64-bitowy
- Alt Workstation 9.2 32-bitowy/64-bitowy
- Alt Workstation 10 32-bitowy/64-bitowy
- Alt 8 SP Server (LKNV.11100-01) 64-bitowy
- Alt 8 SP Server (LKNV.11100-02) 64-bitowy
- Alt 8 SP Server (LKNV.11100-03) 64-bitowy
- Alt 8 SP Workstation (LKNV.11100-01) 32-bitowy/64-bitowy
- Alt 8 SP Workstation (LKNV.11100-02) 32-bitowy/64-bitowy
- Alt 8 SP Workstation (LKNV.11100-03) 32-bitowy/64-bitowy
- Mageia 4 32-bitowy
- Oracle Linux 7 64-bitowy
- Oracle Linux 8 64-bitowy
- Oracle Linux 9 64-bitowy
- Linux Mint 19.x 32-bitowy
- Linux Mint 20.x 64-bitowy
- AlterOS 7.5 i nowszy 64-bitowy
- GosLinux IC6 64-bitowy
- RED OS 7.3 64-bitowy
- RED OS 7.3 Server 64-bitowy
- RED OS 7.3 Certified Edition 64-bitowy
- ROSA COBALT 7.9 64-bitowy
- ROSA CHROME 12 64-bitowy
- Lotos (rdzeń Linux w wersji 4.19.50, DE: MATE) 64-bitowy

- macOS Sierra (10.12)
- macOS High Sierra (10.13)
- macOS Mojave (10.14)
- macOS Catalina (10.15)
- macOS Big Sur (11.x)
- macOS Monterey (12.x)

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

Obsługiwane są następujące platformy wirtualizacji:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64-bitowy
- Microsoft Hyper-V Server 2012 R2 64-bitowy
- Microsoft Hyper-V Server 2016 64-bitowy
- Microsoft Hyper-V Server 2019 64-bitowy
- Microsoft Hyper-V Server 2022 64-bitowy
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Maszyna wirtualna oparta na jądrze jest obsługiwana w przypadku następujących systemów operacyjnych zalecanych do wirtualizacji Kaspersky Security Center:
  - Alt 8 SP Server (LKNV.11100-01) 64-bitowy
  - Alt Server 10 64-bitowy
  - Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7.2 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy) 64-bitowy
  - Debian GNU/Linux 11.x (Bullseye) 32-bitowy/64-bitowy
  - Ubuntu Server 20.04 LTS (Focal Fossa) 64-bitowy
  - RED OS 7.3 64-bitowy
  - RED OS 7.3 Server 64-bitowy
  - RED OS 7.3 Certified Edition 64-bitowy

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

Przed zainstalowaniem Agenta sieciowego na urządzeniach z systemem Windows 7, Windows Server 2008 lub Windows Small Business Server 2011 Premium upewnij się, że zainstalowano aktualizację zabezpieczeń systemu Windows 7 (KB3063858).

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

Możesz zainstalować lub zaktualizować Network Agent for Windows XP tylko w systemie Microsoft Windows XP.

Zalecamy zainstalowanie tej samej wersji Agenta sieciowego dla systemu Linux, co Kaspersky Security Center.

Agent sieciowy dla systemu macOS jest dostarczany wraz z aplikacjami zabezpieczającymi Kaspersky dla tych systemów operacyjnych.

Nieobsługiwane systemy operacyjne i platformy

Serwer administracyjny

Serwer administracyjny nie jest kompatybilny z następującymi systemami operacyjnymi:

- Microsoft Windows Embedded POSReady 2009 z najnowszym pakietem Service Pack 32-bitowy
- Microsoft Windows Embedded POSReady 7 32-/64-bitowy
- Microsoft Windows Embedded Standard 7 z pakietem Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Standard 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Industry Pro 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Industry Enterprise 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Pro 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Update 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 2015 LTSB 32-bitowy/64-bitowy

- Microsoft Windows 10 Enterprise 2016 LTSB 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 2019 LTSC 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-bitowy/ARM
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-bitowy/ARM
- Microsoft Windows 10 IoT Enterprise version 1703 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1709 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1803 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1809 32-bitowy/64-bitowy
- Microsoft Windows 10 20H2 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 21H2 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1909 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1607 32-bitowy/64-bitowy
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Home Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy
- Microsoft Windows 10 Home RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy

- Microsoft Windows 10 Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS1 (aktualizacja rocznicowa, 1607) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Home RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS3 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS3 32-bitowy
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS4 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS4 32-bitowy
- Microsoft Windows 10 Home RS5 (aktualizacja z października 2018 r., 1809) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bitowy/64-bitowy

- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS5 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS5 32-bitowy
- Microsoft Windows 10 Home 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-bitowy/64-bitowy

- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 11 Home 64-bitowy
- Microsoft Windows 11 Pro 64-bitowy
- Microsoft Windows 11 Enterprise 64-bitowy
- Microsoft Windows 11 Education 64-bitowy
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 8.1 Pro 32-bitowy/64-bitowy
- Microsoft Windows 8 (Core) 32-bitowy/64-bitowy
- Microsoft Windows 8 Pro 32-bitowy/64-bitowy
- Microsoft Windows 8 Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate 32-bitowy/64-bitowy
- Microsoft Windows 7 Home Basic/Premium 32-bitowy/64-bitowy
- Microsoft Windows 7 Home Basic/Premium z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows XP Professional z Service Pack 3 i nowszy, 32-bitowy
- Microsoft Windows XP Professional z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Microsoft Windows XP Home Service Pack 3 i wyższy 32-bitowy
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-bitowy
- Windows Essential Business Server 2008 Standard 64-bitowy

- Windows Essential Business Server 2008 Premium 64-bitowy
- Windows Small Business Server 2003 Standard z Service Pack 1 32-bitowy
- Windows Small Business Server 2003 Premium z Service Pack 1 32-bitowy
- Windows Small Business Server 2008 Standard 64-bitowy
- Windows Small Business Server 2008 Premium 64-bitowy
- Windows Small Business Server 2011 Essentials 64-bitowy
- Windows Small Business Server 2011 Premium Add-on 64-bitowy
- Windows Small Business Server 2011 Standard 64-bitowy
- Windows Home Server 2011 64-bitowy
- Windows MultiPoint Server 2010 Standard 64-bitowy
- Windows MultiPoint Server 2010 Premium 64-bitowy
- Windows MultiPoint Server 2011 Standard 64-bitowy
- Windows MultiPoint Server 2011 Premium 64-bitowy
- Windows MultiPoint Server 2012 Standard 64-bitowy
- Windows MultiPoint Server 2012 Premium 64-bitowy
- Microsoft Windows 2000 Server 32-bitowy
- Windows Server 2003 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 Datacenter Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Foundation z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 Service Pack 1 Server Core 32-bitowy/64-bitowy
- Windows Server 2008 Standard Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Standard 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise 32-bitowy/64-bitowy
- Windows Server 2008 Datacenter 32-bitowy/64-bitowy

- Windows Server 2008 z dodatkiem Service Pack 2 (wszystkie wersje) 32-bitowy/64-bitowy
- Windows Server 2008 R2 Server Core 64-bitowy
- Windows Server 2008 R2 Datacenter 64-bitowy
- Windows Server 2008 R2 Datacenter z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Enterprise 64-bitowy
- Windows Server 2008 R2 Enterprise z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Foundation 64-bitowy
- Windows Server 2008 R2 Foundation z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Core Mode z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Standard 64-bitowy
- Windows Server 2016 Nano (Opcja instalacji) (CBB) 64-bitowy
- Windows Server 2016 Server Datacenter RS3 (1709) (LTSB/CBB) 64-bitowy
- Windows Server 2016 Server Standard RS3 (1709) (LTSB/CBB) 64-bitowy
- Windows Server 2016 Server Core RS3 (1709) (Opcja instalacji) (LTSB/CBB) 64-bitowy
- Windows Server 2016 Nano RS3 (1709) (Opcja instalacji) (CBB) 64-bitowy
- Windows Storage Server 2008 32-bitowy/64-bitowy
- Windows Storage Server 2008 Service Pack 2 64-bitowy
- Windows Storage Server 2008 R2 64-bitowy

Serwer bazy danych:

- PostgreSQL 15 64-bitowy
- PostgreSQL Pangolin 64-bitowy
- Microsoft SQL Server 2005 Express 32-bitowy
- Microsoft SQL Server 2005 (wszystkie wersje) 32-bitowy/64-bitowy
- Microsoft SQL Server 2008 Express 32-bitowy
- Microsoft SQL Server 2008 (wszystkie wersje) 32-bitowy/64-bitowy
- Microsoft SQL Server 2008 R2 (wszystkie wersje) 64-bitowy
- Microsoft SQL Server 2008 R2 Service Pack 2 (wszystkie wersje) 64-bitowy
- Microsoft SQL Server 2012 (wszystkie wersje) 64-bitowy

- MySQL 5.0 32-bitowy/64-bitowy
- MySQL Enterprise 5.0 32-bitowy/64-bitowy
- MySQL Standard Edition 5.5 32-bitowy/64-bitowy
- MySQL Enterprise Edition 5.5 32-bitowy/64-bitowy
- MySQL Standard Edition 5.6 32-bitowy/64-bitowy
- MySQL Enterprise Edition 5.6 32-bitowy/64-bitowy
- MySQL Standard Edition 5.7 32-bitowy/64-bitowy
- MySQL Enterprise Edition 5.7 32-bitowy/64-bitowy
- MySQL 5.6 Community 32-bitowy/64-bitowy
- MariaDB Galera Cluster 10.4 32-bitowy/64-bitowy

Następujące platformy wirtualizacji nie są obsługiwane:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro
- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64-bitowy
- Microsoft Hyper-V Server 2008 R2 64-bitowy
- Microsoft Hyper-V Server 2008 R2 z Service Pack 1 i nowszy 64-bitowy
- Microsoft Virtual PC 2007 (6.0.156.0) 32-bitowy/64-bitowy
- Citrix XenServer 5.6

- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7
- Parallels Desktop 7
- Parallels Desktop 11
- Parallels Desktop 14
- Parallels Desktop 16
- Oracle VM VirtualBox 4.0.4-70112 (tylko podczas logowania jako gość systemu Windows)
- Oracle VM VirtualBox 5.x (tylko podczas logowania jako gość systemu Windows)

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console Server

Kaspersky Security Center Web Console Server nie jest kompatybilny z systemami operacyjnymi:

- Microsoft Windows:
  - Microsoft Windows Embedded POSReady 2009 z najnowszym pakietem Service Pack 32-bitowy
  - Microsoft Windows Embedded POSReady 7 32-/64-bitowy
  - Microsoft Windows Embedded Standard 7 z pakietem Service Pack 1 32-bitowy/64-bitowy
  - Microsoft Windows Embedded 8 Standard 32-bitowy/64-bitowy
  - Microsoft Windows Embedded 8 Industry Pro 32-bitowy/64-bitowy
  - Microsoft Windows Embedded 8 Industry Enterprise 32-bitowy/64-bitowy
  - Microsoft Windows Embedded 8.1 Industry Pro 32-bitowy/64-bitowy
  - Microsoft Windows Embedded 8.1 Industry Enterprise 32-bitowy/64-bitowy
  - Microsoft Windows Embedded 8.1 Industry Update 32-bitowy/64-bitowy
  - Microsoft Windows 10 Enterprise 2015 LTSB 32-bitowy/64-bitowy
  - Microsoft Windows 10 Enterprise 2016 LTSB 32-bitowy/64-bitowy
  - Microsoft Windows 10 Enterprise 2019 LTSC 32-bitowy/64-bitowy

- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-bitowy/ARM
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-bitowy/ARM
- Microsoft Windows 10 IoT Enterprise version 1703 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1709 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1803 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1809 32-bitowy/64-bitowy
- Microsoft Windows 10 20H2 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 21H2 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1909 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1607 32-bitowy/64-bitowy
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Home Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy
- Microsoft Windows 10 Home RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy

- Microsoft Windows 10 Mobile RS1 (aktualizacja rocznicowa, 1607) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Home RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS3 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS3 32-bitowy
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS4 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS4 32-bitowy
- Microsoft Windows 10 Home RS5 (aktualizacja z października 2018 r., 1809) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS5 (aktualizacja z października 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS5 (aktualizacja z października 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS5 (aktualizacja z października 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS5 (aktualizacja z października 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS5 32-bitowy

- Microsoft Windows 10 Mobile Enterprise RS5 32-bitowy
- Microsoft Windows 10 Home 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H2 (October 2020 Update)
- Microsoft Windows 10 Pro 20H2 (October 2020 Update)
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update)
- Microsoft Windows 10 Education 20H2 (October 2020 Update)
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 11 Home 64-bitowy

- Microsoft Windows 11 Pro 64-bitowy
- Microsoft Windows 11 Enterprise 64-bitowy
- Microsoft Windows 11 Education 64-bitowy
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Pro 32-bitowy/64-bitowy
- Microsoft Windows 8.1 Enterprise 32-bitowy/64-bitowy
- Windows 8 (Core) 32-bitowy/64-bitowy
- Windows 8 Pro 32-bitowy/64-bitowy
- Windows 8 Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate 32-bitowy/64-bitowy
- Microsoft Windows 7 Home Basic/Premium 32-bitowy/64-bitowy
- Microsoft Windows 7 Home Basic/Premium z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows XP Professional z Service Pack 3 i nowszy, 32-bitowy
- Microsoft Windows XP Professional z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Microsoft Windows XP Home Service Pack 3 i wyższy 32-bitowy
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-bitowy
- Windows Essential Business Server 2008 Standard 64-bitowy
- Windows Essential Business Server 2008 Premium 64-bitowy
- Windows Small Business Server 2003 Standard z Service Pack 1 32-bitowy

- Windows Small Business Server 2003 Premium z Service Pack 1 32-bitowy
- Windows Small Business Server 2008 Standard 64-bitowy
- Windows Small Business Server 2008 Premium 64-bitowy
- Windows Small Business Server 2011 Essentials 64-bitowy
- Windows Small Business Server 2011 Premium Add-on 64-bitowy
- Windows Small Business Server 2011 Standard 64-bitowy
- Windows Home Server 2011 64-bitowy
- Windows MultiPoint Server 2010 Standard 64-bitowy
- Windows MultiPoint Server 2010 Premium 64-bitowy
- Windows MultiPoint Server 2011 Standard 64-bitowy
- Windows MultiPoint Server 2011 Premium 64-bitowy
- Windows MultiPoint Server 2012 Standard 64-bitowy
- Windows MultiPoint Server 2012 Premium 64-bitowy
- Microsoft Windows 2000 Server 32-bitowy
- Windows Server 2003 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 Datacenter Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Foundation z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 Service Pack 1 Server Core 32-bitowy/64-bitowy
- Windows Server 2008 Standard Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Standard 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise 32-bitowy/64-bitowy
- Windows Server 2008 Datacenter 32-bitowy/64-bitowy
- Windows Server 2008 z dodatkiem Service Pack 2 (wszystkie wersje) 32-bitowy/64-bitowy
- Windows Server 2008 R2 Server Core 64-bitowy

- Windows Server 2008 R2 Datacenter 64-bitowy
- Windows Server 2008 R2 Datacenter z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Enterprise 64-bitowy
- Windows Server 2008 R2 Enterprise z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Foundation 64-bitowy
- Windows Server 2008 R2 Foundation z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Core Mode z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Standard 64-bitowy
- Windows Server 2008 R2 Standard z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Service Pack 1 (wszystkie wersje) 64-bitowy
- Windows Server 2016 Nano (Opcja instalacji) (CBB) 64-bitowy
- Windows Server 2016 Server Datacenter RS3 (1709) (LTSB/CBB) 64-bitowy
- Windows Server 2016 Server Standard RS3 (1709) (LTSB/CBB) 64-bitowy
- Windows Server 2016 Server Core RS3 (1709) (Opcja instalacji) (LTSB/CBB) 64-bitowy
- Windows Server 2016 Nano RS3 (1709) (Opcja instalacji) (CBB) 64-bitowy
- Windows Storage Server 2008 32-bitowy/64-bitowy
- Windows Storage Server 2008 Service Pack 2 64-bitowy
- Windows Storage Server 2008 R2 64-bitowy

- Linux:
  - Debian GNU/Linux 7.x (do 7.8) 32-bitowy/64-bitowy
  - Debian GNU/Linux 8.x (Jessie) 32-bitowy/64-bitowy
  - Ubuntu Server 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
  - Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy
  - Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
  - Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy
  - Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bitowy/64-bitowy
  - Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bitowy/64-bitowy
  - CentOS 6.x (do 6.6) 64-bitowy

- CentOS 7.x ARM 64-bitowy
- CentOS 8.x 64-bitowy
- Red Hat Enterprise Linux Server 6.x 32-bitowy/64-bitowy
- SUSE Linux Enterprise Desktop 12 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Desktop 15 (wszystkie pakiety Service Pack) 64-bitowy
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64-bitowy
- openSUSE 15 64-bitowy
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64-bitowy
- Astra Linux Special Edition, wersja 1.7 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy) 64-bitowy
- Astra Linux Special Edition 4.7 ARM
- Alt Workstation 10 32-bitowy/64-bitowy
- Alt 8 SP Workstation (LKNV.11100-01) 32-bitowy/64-bitowy
- Alt 8 SP Workstation (LKNV.11100-02) 32-bitowy/64-bitowy
- Alt 8 SP Workstation (LKNV.11100-03) 32-bitowy/64-bitowy
- Mageia 4 32-bitowy
- Linux Mint 19.x 32-bitowy
- Linux Mint 20.x 64-bitowy
- AlterOS 7.5 i nowszy 64-bitowy
- RED OS 7.3 64-bitowy
- GosLinux IC6 64-bitowy
- ROSA Enterprise Linux Server 7.3 64-bitowy
- ROSA Enterprise Linux Desktop 7.3 64-bitowy
- ROSA COBALT Workstation 7.3 64-bitowy
- ROSA COBALT Server 7.3 64-bitowy
- ROSA COBALT 7.9 64-bitowy
- ROSA CHROME 12 64-bitowy
- Lotos (rdzeń Linux w wersji 4.19.50, DE: MATE) 64-bitowy

Konsola administracyjna

Konsola administracyjna nie jest kompatybilna z następującymi systemami operacyjnymi:

- Microsoft Windows Embedded POSReady 2009 z najnowszym pakietem Service Pack 32-bitowy
- Microsoft Windows Embedded POSReady 7 32-/64-bitowy
- Microsoft Windows Embedded Standard 7 z pakietem Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Standard 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Industry Pro 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Industry Enterprise 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Pro 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8.1 Industry Update 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 2015 LTSB 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 2016 LTSB 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-bitowy/ARM
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-bitowy/ARM
- Microsoft Windows 10 Enterprise 2019 LTSC 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1703 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1709 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1803 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1809 32-bitowy/64-bitowy
- Microsoft Windows 10 20H2 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 21H2 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1909 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32-bitowy/64-bitowy
- Microsoft Windows 10 IoT Enterprise version 1607 32-bitowy/64-bitowy
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-bitowy/64-bitowy

- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Home Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy
- Microsoft Windows 10 Home RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS1 (aktualizacja rocznicowa, 1607) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Home RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS3 (Fall Creators Update, 1709) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS3 32-bitowy

- Microsoft Windows 10 Mobile Enterprise RS3 32-bitowy
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro Mobile Enterprise RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS4 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS4 32-bitowy
- Microsoft Windows 10 Home RS5 (aktualizacja z października 2018 r., 1809) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS5 (aktualizacja z października 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations RS5 (aktualizacja z października 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS5 (aktualizacja z października 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS5 (aktualizacja z października 2018 r.) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS5 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS5 32-bitowy
- Microsoft Windows 10 Home 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H1 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro for Workstations 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 19H2 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-bitowy/64-bitowy

- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 20H2 (October 2020 Update)
- Microsoft Windows 10 Pro 20H2 (October 2020 Update)
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update)
- Microsoft Windows 10 Education 20H2 (October 2020 Update)
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-bitowy/64-bitowy
- Microsoft Windows 11 Home 64-bitowy
- Microsoft Windows 11 Pro 64-bitowy
- Microsoft Windows 11 Enterprise 64-bitowy
- Microsoft Windows 11 Education 64-bitowy
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Pro 32-bitowy/64-bitowy
- Microsoft Windows 8.1 Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 8 Pro 32-bitowy/64-bitowy
- Microsoft Windows 8 (Core) 32-bitowy/64-bitowy
- Microsoft Windows 8 Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate 32-bitowy/64-bitowy
- Microsoft Windows 7 Home Basic/Premium 32-bitowy/64-bitowy

- Microsoft Windows 7 Home Basic/Premium z pakietem Service Pack 1 i nowszy, 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows XP Professional z Service Pack 3 i nowszy, 32-bitowy
- Microsoft Windows XP Professional z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Microsoft Windows XP Home Service Pack 3 i wyższy 32-bitowy
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-bitowy
- Windows Essential Business Server 2008 Standard 64-bitowy
- Windows Essential Business Server 2008 Premium 64-bitowy
- Windows Small Business Server 2003 Standard z Service Pack 1 32-bitowy
- Windows Small Business Server 2003 Premium z Service Pack 1 32-bitowy
- Windows Small Business Server 2008 Standard 64-bitowy
- Windows Small Business Server 2008 Premium 64-bitowy
- Windows Small Business Server 2011 Essentials 64-bitowy
- Windows Small Business Server 2011 Premium Add-on 64-bitowy
- Windows Small Business Server 2011 Standard 64-bitowy
- Windows Home Server 2011 64-bitowy
- Windows MultiPoint Server 2010 Standard 64-bitowy
- Windows MultiPoint Server 2010 Premium 64-bitowy
- Windows MultiPoint Server 2011 Standard 64-bitowy
- Windows MultiPoint Server 2011 Premium 64-bitowy
- Windows MultiPoint Server 2012 Standard 64-bitowy
- Windows MultiPoint Server 2012 Premium 64-bitowy
- Microsoft Windows 2000 Server 32-bitowy

- Windows Server 2003 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 Datacenter Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Foundation z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 Service Pack 1 Server Core 32-bitowy/64-bitowy
- Windows Server 2008 Standard Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Standard 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise 32-bitowy/64-bitowy
- Windows Server 2008 Datacenter 32-bitowy/64-bitowy
- Windows Server 2008 z dodatkiem Service Pack 2 (wszystkie wersje) 32-bitowy/64-bitowy
- Windows Server 2008 R2 Server Core 64-bitowy
- Windows Server 2008 R2 Datacenter 64-bitowy
- Windows Server 2008 R2 Datacenter z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Enterprise 64-bitowy
- Windows Server 2008 R2 Enterprise z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Foundation 64-bitowy
- Windows Server 2008 R2 Foundation z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Core Mode z pakietem Service Pack 1 i nowszym 64-bitowym
- Windows Server 2008 R2 Standard 64-bitowy
- Windows Server 2012 Server Core 64-bitowy
- Windows Server 2012 R2 Server Core 64-bitowy
- Windows Server 2016 Server Core (Opcja instalacji) (LTSB) 64-bitowy
- Windows Server 2016 Nano (Opcja instalacji) (CBB) 64-bitowy
- Windows Server 2016 Server Datacenter RS3 (1709) (LTSB/CBB) 64-bitowy
- Windows Server 2016 Server Standard RS3 (1709) (LTSB/CBB) 64-bitowy

- Windows Server 2016 Server Core RS3 (1709) (Opcja instalacji) (LTSB/CBB) 64-bitowy
- Windows Server 2016 Nano RS3 (1709) (Opcja instalacji) (CBB) 64-bitowy
- Windows Server 2019 Core 64-bitowy
- Windows Server 2022 Core 64-bitowy
- Windows Storage Server 2008 32-bitowy/64-bitowy
- Windows Storage Server 2008 Service Pack 2 64-bitowy
- Windows Storage Server 2008 R2 64-bitowy

Agent sieciowy

Następujące systemy operacyjne nie są obsługiwane:

- Microsoft Windows Embedded 8 Industry Pro 32-bitowy/64-bitowy
- Microsoft Windows Embedded 8 Industry Enterprise 32-bitowy/64-bitowy
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-bitowy
- Microsoft Windows 10 Home Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (aktualizacja z listopada 2015 r., 1511) 32-bitowy
- Microsoft Windows 10 Home RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS1 (aktualizacja rocznicowa, 1607) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS1 (aktualizacja rocznicowa, 1607) 32-bitowy

- Microsoft Windows 10 Mobile Enterprise RS1 (aktualizacja rocznicowa, 1607) 32-bitowy
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-bitowy/64-bitowy
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-bitowy
- Microsoft Windows 10 Mobile RS3 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS3 32-bitowy
- Microsoft Windows 10 Mobile RS4 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS4 32-bitowy
- Microsoft Windows 10 Mobile RS5 32-bitowy
- Microsoft Windows 10 Mobile Enterprise RS5 32-bitowy
- Microsoft Windows 8 (Core) 32-bitowy/64-bitowy
- Microsoft Windows 7 Professional 32-bitowy/64-bitowy
- Microsoft Windows 7 Enterprise/Ultimate 32-bitowy/64-bitowy
- Microsoft Windows 7 Home Basic/Premium 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 1 32-bitowy/64-bitowy
- Microsoft Windows Vista Business z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Enterprise z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows Vista Ultimate z Service Pack 2 i nowszy 32-bitowy/64-bitowy
- Microsoft Windows XP Professional z dodatkiem Service Pack 2 32-bitowy/64-bitowy
- Microsoft Windows XP Home Service Pack 3 i wyższy 32-bitowy
- Windows Essential Business Server 2008 Standard 64-bitowy
- Windows Essential Business Server 2008 Premium 64-bitowy
- Windows Small Business Server 2003 Standard z Service Pack 1 32-bitowy

- Windows Small Business Server 2003 Premium z Service Pack 1 32-bitowy
- Windows Small Business Server 2008 Standard 64-bitowy
- Windows Small Business Server 2008 Premium 64-bitowy
- Windows Home Server 2011 64-bitowy
- Windows MultiPoint Server 2010 Standard 64-bitowy
- Windows MultiPoint Server 2010 Premium 64-bitowy
- Microsoft Windows 2000 Server 32-bitowy
- Windows Server 2003 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Enterprise z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2003 R2 Standard z Service Pack 2 32-bitowy/64-bitowy
- Windows Server 2008 Datacenter Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Service Pack 1 Server Core 32-bitowy/64-bitowy
- Windows Server 2008 Standard Service Pack 1 32-bitowy/64-bitowy
- Windows Server 2008 Standard 32-bitowy/64-bitowy
- Windows Server 2008 Enterprise 32-bitowy/64-bitowy
- Windows Server 2008 Datacenter 32-bitowy/64-bitowy
- Windows Server 2008 R2 Server Core 64-bitowy
- Windows Server 2008 R2 Datacenter 64-bitowy
- Windows Server 2008 R2 Enterprise 64-bitowy
- Windows Server 2008 R2 Foundation 64-bitowy
- Windows Server 2008 R2 Standard 64-bitowy
- Windows Server 2016 Nano (Opcja instalacji) (CBB)
- Windows Storage Server 2008 32-bitowy/64-bitowy
- Windows Storage Server 2008 Service Pack 2 64-bitowy
- Windows Storage Server 2008 R2 64-bitowy
- Debian GNU/Linux 7.x (do 7.8) 32-bitowy/64-bitowy

- Debian GNU/Linux 8.x (Jessie) 32-bitowy/64-bitowy
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-bitowy/64-bitowy
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-bitowy/64-bitowy
- CentOS 6.x (do 6.6) 64-bitowy
- CentOS 8.x 64-bitowy
- Red Hat Enterprise Linux Server 6.x 32-bitowy/64-bitowy
- SUSE Linux Enterprise Desktop 12 (wszystkie SP) 64-bitowy
- Astra Linux Special Edition, wersja 1.7 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy) 64-bitowy
- Astra Linux Special Edition 4.7 ARM
- ROSA Enterprise Linux Server 7.3 64-bitowy
- ROSA Enterprise Linux Desktop 7.3 64-bitowy
- ROSA COBALT Workstation 7.3 64-bitowy
- ROSA COBALT Server 7.3 64-bitowy
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)

Następujące platformy wirtualizacji nie są obsługiwane:

- VMware vSphere 4.1
- VMware vSphere 5.0
- VMware vSphere 5.1
- VMware vSphere 5.5
- VMware vSphere 6
- VMware vSphere 6.5
- VMware Workstation 9.x
- VMware Workstation 10.x
- VMware Workstation 11.x
- VMware Workstation 12.x Pro

- VMware Workstation Pro 14
- VMware Workstation Pro 15
- Microsoft Hyper-V Server 2008 64-bitowy
- Microsoft Hyper-V Server 2008 R2 64-bitowy
- Microsoft Hyper-V Server 2008 R2 z Service Pack 1 i nowszy 64-bitowy
- Citrix XenServer 6.0
- Citrix XenServer 6.1
- Citrix XenServer 6.2
- Citrix XenServer 6.5
- Citrix XenServer 7

Lista obsługiwanych aplikacji i rozwiązań firmy Kaspersky

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

Lista rozwiązań i aplikacji firmy Kaspersky obsługiwanych przez Kaspersky Security Center

Nazwa aplikacji lub rozwiązania firmy Kaspersky	Obsługiwane przez Konsolę administracyjną opartą na konsoli MMC	Obsługiwane przez Kaspersky Security Center Web Console
Dla stacji roboczych		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security for Linux ARM Edition	✓	✓
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Do rozwiązań przemysłowych		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for	✓	✓

Networks (scentralizowana zdalna instalacja nie jest obsługiwana)		
Dla urządzeń mobilnych		
Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	–	✓
Dla serwerów plików		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Dla środowisk wirtualnych		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	–
Dla serwerów poczty i współpracy		
Kaspersky Security for Linux Mail Server	✓	–
Kaspersky Secure Mail Gateway	✓	–
Kaspersky Security for Microsoft Exchange Servers	✓	–
Do wykrywania ataków ukierunkowanych		
Kaspersky Sandbox Server	–	✓
Kaspersky Endpoint Detection and Response Optimum	–	✓
Kaspersky Managed Detection and Response	–	✓
Dla urządzeń KasperskyOS		
Kaspersky IoT Secure Gateway	–	✓
KasperskyOS Thin Client	–	✓

Licencje i funkcje Kaspersky Security Center 14.2

Kaspersky Security Center wymaga licencji dla niektórych swoich funkcji.

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

Licencje i funkcje Kaspersky Security Center

Funkcje Kaspersky Security Center	Zarządzanie lukami i poprawkami Kaspersky	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersk EDR Optimum

Ocena luk	✓	✓	✓	✓	✓	✓	✓
Zarządzanie poprawkami	✓	–	✓	✓	–	✓	✓
Kontrola dostępu oparta o rolę	✓	✓	✓	✓	✓	✓	✓
Instalacja systemów operacyjnych i aplikacji	✓	–	✓	✓	–	✓	✓
Zarządzanie urządzeniami mobilnymi (czyli zarządzanie urządzeniami iOS i Android użytkowników)	✓	✓	✓	✓	–	–	✓
Configure cloud environment do pracy w środowiskach chmury, takich jak AWS, Microsoft Azure lub Google Cloud	–	–	–	–	✓	✓	–
Eksportowanie zdarzeń do systemów SIEM: Syslog	✓	✓	✓	✓	✓	✓	✓
Eksportowanie zdarzeń do systemów SIEM: QRadar firmy IBM i Micro Focus firmy ArcSight	✓	–	✓	✓	–	✓	✓

Informacje o kompatybilności Serwera administracyjnego i Kaspersky Security Center Web Console

Zalecane jest korzystanie z najnowszej wersji Serwera administracyjnego Kaspersky Security Center i Kaspersky Security Center Web Console; w przeciwnym razie funkcjonalność Kaspersky Security Center może być ograniczona.

Możesz niezależnie zainstalować i uaktualnić Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center Web Console. W takim przypadku, musisz upewnić się, że wersja zainstalowanej konsoli Kaspersky Security Center Web Console jest zgodna z wersją Serwera administracyjnego, z którym się łączysz.

- Konsola internetowa Kaspersky Security Center 14.2 Web Console obsługuje serwer administracyjny Kaspersky Security Center w następujących wersjach: 14.2, 14 i 13.2.
- Serwer administracyjny Kaspersky Security Center 14.2 obsługuje Kaspersky Security Center Web Console w następujących wersjach: 14.2, 14 i 13.2.

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

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

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

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

Funkcja lub właściwość	Kaspersky Security Center	
	Rozwiązanie oparte na systemie Windows	**Rozwiązanie oparte na systemie Linux**
Lokalizacja Serwera administracyjnego	Lokalnie	Lokalnie
Lokalizacja systemu zarządzania bazą danych (DBMS)	Lokalnie	Lokalnie
System operacyjny do zainstalowania Serwera administracyjnego	Windows	Linux
Typ konsoli administracyjnej	Lokalne i internetowe	Internetowe
System operacyjny do zainstalowania internetowej konsoli administracyjnej	Windows lub Linux	Windows lub Linux
Hierarchia Serwerów administracyjnych	✓	✓
Hierarchia Grupy administracyjnej	✓	✓
Przeszukiwanie sieci	✓	✓ (tylko według zakresów IP)
Maksymalna liczba zarządzanych urządzeń	100 000	20 000
Ochrona urządzeń zarządzanych przez systemy Windows, macOS i Linux	✓	✓ (tylko ochrona urządzeń z systemem Linux i Windows)
Ochrona urządzeń mobilnych	✓	–
Ochrona maszyn wirtualnych	✓	–
Ochrona infrastruktury chmury publicznej	✓	–

Zarządzanie bezpieczeństwem zorientowane na urządzenie	✓	✓
Zarządzanie bezpieczeństwem zorientowane na użytkownika	✓	✓
Zasady aplikacji	✓	✓
Zadania dla aplikacji Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
KSN Proxy	✓	✓
Kaspersky Private Security Network	✓	✓
Scentralizowane wdrażanie kluczy licencyjnych dla aplikacji Kaspersky	✓	✓
Obsługa wirtualnych Serwerów administracyjnych	✓	✓
Instalowanie aktualizacji oprogramowania firm trzecich i naprawianie luk w zabezpieczeniach oprogramowania firm trzecich	✓	– (tylko przy użyciu zadania zdalnej instalacji)
Powiadomienia o zdarzeniach, które miały miejsce na zarządzanych urządzeniach	✓	✓
Tworzenie i zarządzanie kontami użytkowników	✓	✓
Monitorowanie statusu polityk i zadań	✓	✓
Wdrażanie klastra trybu failover Kaspersky	✓	✓
Używanie SNMP do wysyłania statystyk Serwera administracyjnego do aplikacji innych firm	✓	–
Zdalna diagnostyka urządzeń klienckich	✓	–
Zdalne połączenie z pulpitem urządzenia klienckiego	✓	–
Automatyczna aktualizacja antywirusowych baz danych	✓	✓
Automatyczna aktualizacja aplikacji Kaspersky	✓	–
Instalacja systemów operacyjnych na urządzeniach klienckich	✓	–
Serwer WWW do publikowania pakietów instalacyjnych i innych plików	✓	–
Zarządzanie licencjami stron trzecich	✓	–

Informacje o Kaspersky Security Center Cloud Console

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

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

Interfejs i dokumentacja Kaspersky Security Center Cloud Console są dostępne w następujących językach:

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

Więcej informacji o konsoli Kaspersky Security Center Cloud Console i jej funkcjach można znaleźć w dokumentacji do Kaspersky Security Center Cloud Console oraz w dokumentacji do Kaspersky Endpoint Security for Business.

Podstawowe pojęcia

Ta sekcja wyjaśnia podstawowe pojęcia związane z Kaspersky Security Center.

Serwer administracyjny

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

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

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

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

Serwer administracyjny pełni następujące funkcje:

- Przechowuje strukturę grup administracyjnych
- Przechowuje informacje o konfiguracji urządzeń klienckich
- Organizuje repozytoria dla pakietów dystrybucyjnych aplikacji
- Służy do zdalnej instalacji aplikacji na urządzeniach klienckich oraz do usuwania aplikacji
- Aktualizuje bazy danych i moduły aplikacji firmy Kaspersky
- Zarządza profilami i zadaniami na urządzeniach klienckich
- Przechowuje informacje o zdarzeniach, które wystąpiły na urządzeniach klienckich
- Generuje raporty z działania aplikacji Kaspersky
- Rozsyła klucze licencyjne do urządzeń klienckich oraz przechowuje informacje o kluczach licencyjnych
- Wysyła komunikaty o postępie zadań (na przykład o wykryciu wirusów na urządzeniu klienckim)

Nadawanie nazw Serwerom administracyjnym w interfejsie aplikacji

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

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

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

Hierarchia Serwerów administracyjnych

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

Wirtualne Serwery administracyjne są szczególnym przypadkiem podrzędnych Serwerów administracyjnych.

Hierarchii Serwerów administracyjnych można użyć w celu:

- Zmniejszenia obciążenia na Serwerze administracyjnym (w porównaniu do pojedynczego Serwera działającego dla całej sieci).

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

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

- Sposób wykorzystania Kaspersky Security Center przez dostawców usługi. Dostawca usługi musi tylko zainstalować Kaspersky Security Center i Kaspersky Security Center Web Console. Aby zarządzać dużą liczbą urządzeń klienckich w różnych organizacjach, dostawca usługi może dodać wirtualne Serwery administracyjne do hierarchii Serwerów administracyjnych.

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

Wirtualny Serwer administracyjny

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

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

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

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

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

Dodatkowo, wirtualny Serwer administracyjny posiada następujące ograniczenia:

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

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

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

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

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

Serwer urządzeń mobilnych

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

Istnieją dwa typy serwerów urządzeń mobilnych:

- Serwer urządzeń mobilnych Exchange. Serwer jest instalowany na urządzeniu, na którym zainstalowano serwer Microsoft Exchange. Umożliwia on pobieranie danych z serwera Microsoft Exchange i przesyłanie ich do Serwera administracyjnego. Ten serwer urządzeń mobilnych jest używany do zarządzania urządzeniami mobilnymi, które obsługują protokół Exchange ActiveSync.

- Serwer iOS MDM. Ten serwer urządzeń mobilnych jest używany do zarządzania urządzeniami mobilnymi, które obsługują usługę Apple® Push Notification (APNs).

Serwery urządzeń mobilnych Kaspersky Security Center umożliwiają zarządzanie następującymi obiektami:

- Pojedynczym urządzeniem mobilnym.

- Kilkoma urządzeniami mobilnymi.

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

Serwer sieciowy

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

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

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

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

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

Składnia odnośnika do przesłania informacji wygląda następująco:

`https://<nazwa serwera sieciowego>:<port HTTPS>/public/<obiekt>,`

gdzie:

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

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

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

Agent sieciowy

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

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

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

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

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

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

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

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

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

Grupy administracyjne

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

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

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

Zarządzane urządzenie może należeć tylko do jednej grupy administracyjnej.

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

Zarządzane urządzenie

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

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

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

Urządzenie nieprzypisane

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

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

Stacja robocza administratora

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

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

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

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

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

Wtyczka administracyjna

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

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

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

Wtyczki do zarządzania można pobrać ze strony pomocy technicznej Kaspersky.

Sieciowa wtyczka administracyjna

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

Wtyczki sieciowe do zarządzania można pobrać ze strony internetowej pomocy technicznej Kaspersky.

Wtyczka zarządzająca oferuje:

- Interfejs do tworzenia i edytowania zadań i ustawień aplikacji
- Interfejs do tworzenia i edytowania zasad i profili zasad do zdalnej i scentralizowanej konfiguracji aplikacji Kaspersky i urządzeń

- Przesyłanie zdarzeń wygenerowanych przez aplikację
- Funkcje Kaspersky Security Center Web Console do wyświetlania danych operacyjnych i zdarzeń aplikacji, a także statystyk przekazanych z urządzeń klienckich

Zasady

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

Stan zasady

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

Zasady działają zgodnie z następującymi regułami:

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

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

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

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

Profile zasad działają zgodnie z następującymi regułami:

- Profil zasad zaczyna obowiązywać, gdy wystąpi określony warunek aktywacji.
- Profile zasad zawierają wartości ustawień, które różnią się od ustawień zasad.
- Aktywacja profilu zasad zmienia obowiązujące ustawienia zarządzanego urządzenia.

- Zasada może zawierać maksymalnie 100 profili zasad.

Profile zasad

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

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

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

Zadania

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

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

Zadania mogą być wykonywane na Serwerze administracyjnym i na urządzeniach.

Na Serwerze administracyjnym wykonywane są następujące zadania:

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

Na urządzeniach wykonywane są następujące typy zadań:

- *Zadania lokalne*—zadania wykonywane na określonym urządzeniu

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

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

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

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

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

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

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

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

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

Obszar zadania

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

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

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

- Ręcznie określ pewne urządzenia.

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

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

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

- Utwórz wybór urządzeń.

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

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

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

Jak ustawienia lokalne aplikacji mają się do zasad

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

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

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

- Jeśli modyfikacja ustawienia jest zablokowana, wówczas ta sama wartość (określona w profilu) używana jest na wszystkich urządzeniach klienckich.
- Jeśli modyfikacja ustawienia jest odblokowana, wówczas na każdym urządzeniu klienckim aplikacja używa wartości lokalnej zamiast wartości określonej w profilu. W takiej sytuacji ustawienie może być zmieniane w lokalnych ustawieniach aplikacji.

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

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

Lokalne ustawienia aplikacji są zmieniane po pierwszym zastosowaniu profilu w zgodzie z jego ustawieniami.

Punkt dystrybucji

Punkt dystrybucji (wcześniej znany jako agent aktualizacji) to urządzenie z zainstalowanym Agentem sieciowym, które jest używane do dystrybucji aktualizacji, zdalnej instalacji aplikacji oraz pobierania informacji o urządzeniach w sieci. Punkt dystrybucji może wykonywać następujące funkcje:

- Rozsyłaj uaktualnienia i pakiety instalacyjne pobrane z Serwera administracyjnego na urządzenia klienckie w grupie (włączając w to taką metodę, jak multicasting z użyciem protokołu UDP). Uaktualnienia mogą być pobierane z Serwera administracyjnego lub z serwerów aktualizacji Kaspersky. W drugim przypadku należy utworzyć zadanie dla punktu dystrybucji.

Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky.

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

Punkty dystrybucji przyspieszają rozsyłanie uaktualnień i zwalniają zasoby Serwera administracyjnego.

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

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

  Obecność punktu dystrybucji, który działa jako brama połączenia, nie blokuje opcji bezpośredniego połączenia pomiędzy zarządzanymi urządzeniami a Serwerem administracyjnym. Jeśli brama połączenia nie jest dostępna, ale bezpośrednie połączenie z Serwerem administracyjnym jest technicznie możliwe, zarządzane urządzenia zostaną połączone bezpośrednio z Serwerem administracyjnym.
- Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może stosować te same metody wykrywania urządzeń co Serwer administracyjny.
- Wykonaj zdalną instalację oprogramowania firm trzecich i aplikacji firmy Kaspersky przy użyciu narzędzi systemu operacyjnego punktu dystrybucji. Należy pamiętać, że punkt dystrybucji może przeprowadzić instalację na urządzeniach klienckich bez Agenta sieciowego.

  Ta funkcja umożliwia zdalne przesłanie pakietów instalacyjnych Agenta sieciowego na urządzenia klienckie znajdujące się w sieciach, do których Serwer administracyjny nie ma bezpośredniego dostępu.
- Pełnienie funkcji serwera proxy uczestniczącego w Kaspersky Security Network(KSN).

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

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

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

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

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

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

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

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

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

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

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

Punkt dystrybucji wymaga przynajmniej 4 GB wolnej przestrzeni na dysku. Jeśli przestrzeń na dysku punktu dystrybucji jest mniejsza niż 2 GB, Kaspersky Security Center tworzy zdarzenie z poziomem istotności *Ostrzeżenie*. Zdarzenie zostanie opublikowane we właściwościach urządzenia, w sekcji **Zdarzenia**.

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

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

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

Brama połączenia

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

Brama połączenia może komunikować się z maksymalnie 10 000 urządzeń.

Masz dwie możliwości korzystania z bram połączeń:

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

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

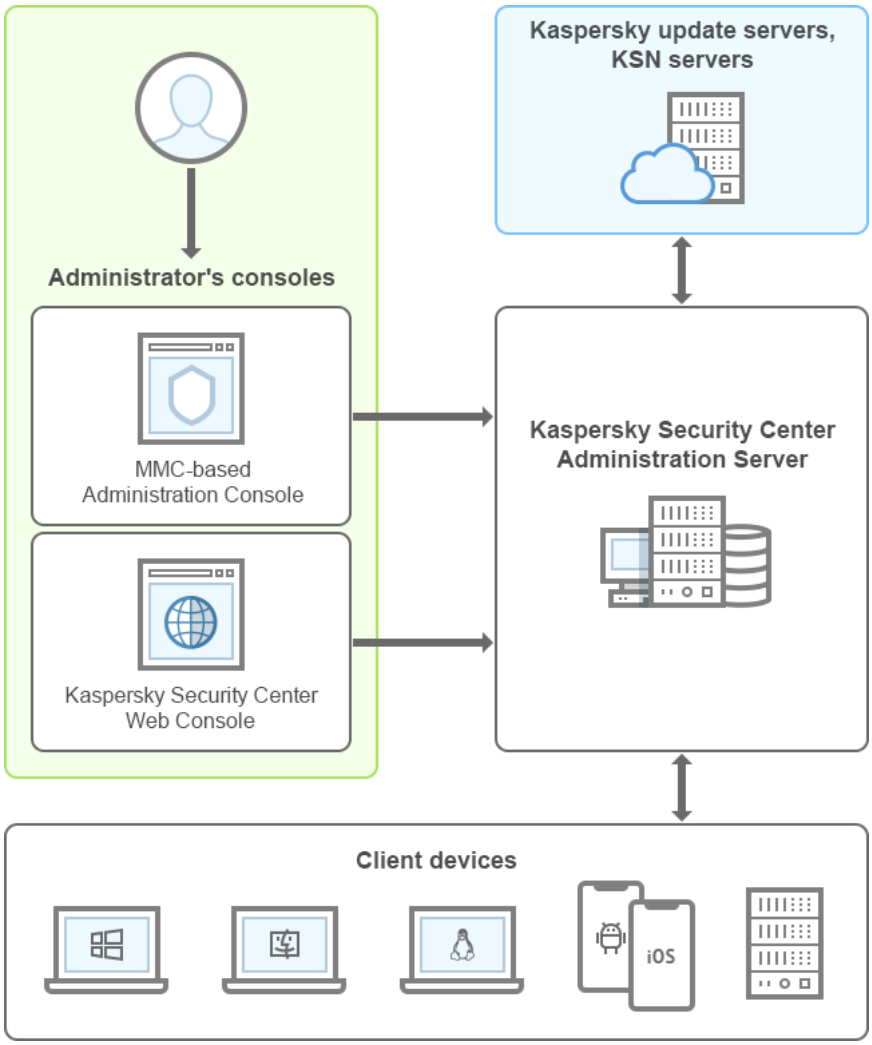
  Brama połączenia nie może nawiązać połączenia z Serwerem administracyjnym przez inną bramę połączenia. Oznacza to, że Agent sieciowy nie może być jednocześnie bramą połączenia i używać bramy połączenia do łączenia się z Serwerem administracyjnym.

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

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

Architektura

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



Architektura Kaspersky Security Center

Kaspersky Security Center zawiera następujące główne moduły:

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

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

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

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

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

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

Główny scenariusz instalacji

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

Więcej informacji o wdrożeniu konsoli Kaspersky Security Center Cloud Console można znaleźć w dokumentacji do Kaspersky Security Center Cloud Console.

Instalacja Kaspersky Security Center składa się na następujące etapy:

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

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

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

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

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

Instalacja Kaspersky Security Center odbywa się w krokach:

Prace przygotowawcze

1 **Pobieranie niezbędnych plików**

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

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

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

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

2 Wybieranie struktury ochrony organizacji

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

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

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

Jeśli musisz zapewnić ochronę urządzeń mobilnych, przeprowadź wszystkie wstępnie wymagane działania niezbędne dla konfiguracji serwera urządzeń mobilnych Exchange i serwera iOS MDM.

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

3 Przygotowanie do użycia certyfikatów niestandardowych

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

4 Przygotowanie do licencjonowania Kaspersky Security Center

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

5 Przygotowanie do licencjonowania zarządzanych aplikacji zabezpieczających

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

6 Wybieranie konfiguracji sprzętowej Serwera administracyjnego i systemu DBMS

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

7 Wybieranie systemu zarządzania bazą danych

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

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

8. **Instalowanie systemu DBMS i tworzenie bazy danych**

   Zapoznaj się z informacjami na temat kont do pracy z DBMS i zainstaluj swój system DBMS. Zanotuj na kartce, a następnie zapisz ustawienia DBMS, ponieważ będziesz ich potrzebował podczas instalacji Serwera administracyjnego. Te ustawienia obejmują nazwę serwera SQL, numer portu używanego do łączenia z serwerem SQL, nazwę konta i hasło do uzyskania dostępu do serwera SQL.

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

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

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

9. **Konfigurowanie portów**

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

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

10. **Sprawdzanie kont**

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

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

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

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

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

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

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

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

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

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

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

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

2. **Wstępna konfiguracja i licencjonowanie**

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

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

3. **Sprawdzanie, czy instalacja Serwera administracyjnego została zakończona pomyślnie**

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

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

   Po zakończeniu sprawdzania, przejdź do kroków poniżej.

Scentralizowane wdrażanie aplikacji zabezpieczających Kaspersky na urządzeniach klienckich

1. **Wykrywanie urządzeń w sieci**

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

2 Instalowanie Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci

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

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

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

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

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

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

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

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

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

3 Rozsyłanie kluczy licencyjnych na urządzenia klienckie

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

4 Konfigurowanie ochrony urządzeń mobilnych

Ten krok jest częścią kreatora wstępnej konfiguracji.

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

5 Tworzenie struktury grupy administracyjnej

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

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

6 Przypisywanie punktów dystrybucji

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

Porty używane przez Kaspersky Security Center

Poniżej znajduje się tabela zawierająca domyślne porty, które muszą być otwarte na Serwerach administracyjnych i urządzeniach klienckich. Jeśli chcesz, możesz zmienić domyślne numery portów.

Poniżej znajduje się tabela zawierająca domyślne porty, które muszą być otwarte na Serwerze administracyjnym. Jednakże jeśli instalujesz Serwer administracyjny i bazę danych na różnych urządzeniach, musisz udostępnić potrzebne porty na urządzeniu, na którym znajduje się baza danych (na przykład: port 3306 dla MySQL Server i MariaDB Server, port 1433 dla Microsoft SQL Server, lub port 5432 dla PostgreSQL i Postgres Pro). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

Porty, które muszą być otwarte na Serwerze administracyjnym

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
8060	klcsweb	TCP	Przesyłanie opublikowanych pakietów instalacyjnych na urządzenia klienckie	Publikowanie pakietów instalacyjnych. Możesz zmienić domyślny numer portu w sekcji **Serwera internetowego** okna właściwości Serwera administracyjnego w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
8061	klcsweb	TCP (TLS)	Przesyłanie opublikowanych pakietów instalacyjnych na urządzenia klienckie	Publikowanie pakietów instalacyjnych. Możesz zmienić domyślny numer portu w sekcji **Serwera internetowego** okna właściwości Serwera administracyjnego w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
13000	klserver	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych i podrzędnych Serwerów administracyjnych; używany także na podrzędnych Serwerach administracyjnych do odbierania połączeń od głównego Serwera administracyjnego (na przykład, jeśli podrzędny Serwer administracyjny znajduje się w strefie DMZ)	Zarządzanie urządzeniami klienckimi i podrzędnymi Serwerami administracyjnymi.

				Możesz zmienić numer domyślnego portu do odbierania połączeń od Agentów sieciowych podczas konfigurowania portów połączeń; możesz zmienić numer domyślnego portu do odbierania połączeń z podrzędnych Serwerów administracyjnych podczas tworzenia hierarchii Serwerów administracyjnych w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
13000	klserver	UDP	Pobieranie informacji o urządzeniach, które zostały wyłączone, z Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić numer domyślnego portu w ustawieniach zasad Agenta sieciowego w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
13291	klserver	TCP (TLS)	Odbieranie połączeń od Konsoli administracyjnej do Serwera administracyjnego	Zarządzanie Serwerem administracyjnym. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego w Konsoli administracyjnej.
13299	klserver	TCP (TLS)	Odbieranie połączeń od Kaspersky Security Center Web Console do Serwera administracyjnego; odbieranie połączeń do Serwera administracyjnego poprzez OpenAPI	Kaspersky Security Center Web Console, OpenAPI. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego (w podsekcji **Porty połączeń** sekcji **Ogólne**) w Konsoli administracyjnej lub podczas tworzenia hierarchii Serwerów administracyjnych w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
14000	klserver	TCP	Odbieranie połączeń od Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić numer domyślnego portu, gdy konfigurowanie portów połączeń podczas instalacji Kaspersky Security Center lub podczas ręcznego łączenia urządzenia klienckiego z Serwerem administracyjnym.
13111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	TCP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
15111 (tylko wtedy, gdy	ksnproxy	UDP	Odbieranie żądań od zarządzanych urządzeń do	Serwer KSN proxy.

usługa KSN proxy jest uruchomiona na urządzeniu)			serwera KSN proxy	Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
17000	klactprx	TCP (TLS)	Odbieranie połączeń dla aktywacji aplikacji od zarządzanych urządzeń (za wyjątkiem urządzeń mobilnych)	Serwer proxy aktywacji używany przez urządzenia inne niż mobilne do aktywacji aplikacji Kaspersky za pomocą kodów aktywacyjnych. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
17100 (tylko wtedy, gdy zarządzasz urządzeniami mobilnymi)	klactprx	TCP (TLS)	Odbieranie połączeń dla aktywacji aplikacji od urządzeń mobilnych	Aktywacja przy użyciu serwera proxy dla urządzeń mobilnych. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
19170	klserver	HTTPS (TLS)	Tunelowanie połączeń z zarządzanymi urządzeniami przy użyciu narzędzia klsctunnel	Zdalne nawiązywanie połączenia z zarządzanymi urządzeniami przy użyciu Kaspersky Security Center Web Console. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego (w podsekcji **Dodatkowe porty** sekcji **Ogólne**) tylko w Konsoli administracyjnej.
13292 (tylko wtedy, gdy zarządzasz urządzeniami mobilnymi)	klserver	TCP (TLS)	Obieranie połączeń od urządzeń mobilnych	Zarządzanie urządzeniami mobilnymi. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
13294 (tylko wtedy, gdy zarządzasz urządzeniami mobilnymi)	klserver	TCP (TLS)	Odbieranie połączeń od urządzeń chronionych UEFI	Zarządzanie urządzeniami klienckimi chronionymi UEFI. Możesz zmienić domyślny numer portu podczas podłączania urządzeń mobilnych lub później, w oknie właściwości Serwera administracyjnego (w podsekcji Dodatkowe porty, w sekcji **Ogólne**) w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.

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

Port używany przez Kaspersky Security Center iOS MDM Server

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
443	kliosmdmservicesrv	TCP (TLS)	Obieranie połączeń od urządzeń mobilnych iOS	Zarządzanie urządzeniami mobilnymi.

				Możesz zmienić numer domyślnego portu podczas instalowania serwera iOS MDM.

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

Port używany przez Kaspersky Security Center Web Console Server

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

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

Porty używane przez Agenta sieciowego

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
15000	klnagent	UDP	Sygnały zarządzania z Serwera administracyjnego do Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić numer domyślnego portu w ustawieniach zasad Agenta sieciowego w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
15000	klnagent	Emisja protokołu UDP	Uzyskiwanie danych o innych Agentach sieciowych w obrębie tej samej domeny broadcastowej (dane są następnie wysyłane do Serwera administracyjnego)	Dostarczanie uaktualnień i pakietów instalacyjnych.
15001	klnagent	UDP	Odbieranie żądań multiemisji z punktu dystrybucji (jeśli jest używany)	Odbieranie aktualizacji i pakietów instalacyjnych z punktu dystrybucji. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.

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

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

Porty używane przez Agenta sieciowego pełniącego rolę punktu dystrybucji

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
13000	klnagent	TCP (TLS)	Odbieranie połączeń od Agentów sieciowych	Zarządzanie urządzeniami klienckimi, dostarczanie uaktualnień i pakietów instalacyjnych. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
13111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	TCP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
15111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	UDP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
17111 (tylko wtedy, gdy usługa KSN proxy jest uruchomiona na urządzeniu)	ksnproxy	HTTPS	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.
13295 (tylko wtedy, gdy używasz punktu dystrybucji jako serwera push)	klnagent	TCP (TLS)	Wysyłanie powiadomień typu push na zarządzane urządzenia	Serwer push. Możesz zmienić numer domyślnego portu w oknie właściwości punktu dystrybucji w Konsoli administracyjnej lub w Kaspersky Security Center Web Console.

Certyfikaty do pracy z Kaspersky Security Center

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

Informacje o certyfikatach Kaspersky Security Center

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

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

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

- C – typowy certyfikat dla portów 13000 i 13291
- CR – typowy rezerwowy certyfikat dla portów 13000 i 13291
- M – certyfikat mobilny dla portu 13292
- MR – rezerwowy certyfikat mobilny dla portu 13292
- MCA – mobilny urząd certyfikacji dla automatycznie wygenerowanych certyfikatów użytkowników

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

Certyfikaty Serwera administracyjnego

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

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

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

Certyfikaty mobilne

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

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

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

Certyfikat serwera iOS MDM

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

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

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

Certyfikat Kaspersky Security Center Web Server

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

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

1. Niestandardowy certyfikat serwer sieciowy, który określiłeś ręcznie przy użyciu Konsoli administracyjnej
2. Niestandardowy certyfikat Serwera administracyjnego („C")

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

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

Certyfikat Kaspersky Security Center Web Console

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

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

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

Informacje o certyfikacie Serwera administracyjnego

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

Certyfikat wydany przez Kaspersky

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

Certyfikat Serwera administracyjny jest ważny przez pięć lat, jeśli certyfikat został opublikowany przed 1 września 2020 roku. W przeciwnym razie okres ważności certyfikatu jest ograniczony 397 dni. Nowy certyfikat jest generowany na Serwerze administracyjnym jako zapasowy certyfikat na 90 dni przed datą wygaśnięcia bieżącego certyfikatu. Następnie, nowy certyfikat automatycznie zastępuje bieżący certyfikat dzień przed datą wygaśnięcia. Wszystkie Agenty sieciowe na urządzeniach klienckich są automatycznie ponownie konfigurowane do autoryzacji na Serwerze administracyjnym przy użyciu nowego certyfikatu.

Jeśli dla certyfikatu Serwera administracyjnego określisz okres ważności dłuższy niż 397 dni, przeglądarka zwróci błąd.

Certyfikaty niestandardowe

Jeśli to konieczne, możesz przypisać certyfikat innej firmy dla Serwera administracyjnego. Na przykład, to może być konieczne w celu zapewnienia lepszej integracji z istniejącą PKI Twojej firmy lub w celu przeprowadzenia konfiguracji niestandardowej pól certyfikatu. Podczas zamiany certyfikatu, wszystkie Agenty sieciowe, które wcześniej były połączone z Serwerem administracyjnym za pomocą protokołu SSL, utracą połączenie i zwrócą "Błąd autoryzacji Serwera administracyjnego". Aby wyeliminować ten błąd, będziesz musiał przywrócić połączenie po zastąpieniu certyfikatu.

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

Wymagania dotyczące niestandardowych certyfikatów stosowanych w Kaspersky Security Center

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

Wymagania wobec certyfikatów Kaspersky Security Center

Typ certyfikatu	Wymagania	Komentarze
Wspólny certyfikat, wspólny certyfikat rezerwowy („C”, „CR”)	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie kluczy • Podpisywanie CRL Rozszerzone użycie klucza (opcjonalnie): uwierzytelnianie serwera, uwierzytelnianie klienta.	Parametr Rozszerzone użycie klucza jest opcjonalny. Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak”, ale nie mniejsza niż „1”.
Certyfikat mobilny, mobilny certyfikat rezerwowy („M”, „MR”)	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie kluczy	Parametr Rozszerzone użycie klucza jest opcjonalny. Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak”, jeśli wspólny certyfikat ma wartość ograniczenia długości ścieżki nie mniejszą niż „1”.

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

Scenariusz: Określanie niestandardowego certyfikatu Serwera administracyjnego

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

Jeśli dla certyfikatu Serwera administracyjnego określisz okres ważności dłuższy niż 397 dni, przeglądarka zwróci błąd.

Wymagania wstępne

Nowy certyfikat musi być utworzony w formacie PKCS#12 (na przykład, za pomocą PKI organizacji) i musi być wystawiony przez zaufany urząd certyfikacji (CA). Ponadto nowy certyfikat musi zawierać cały łańcuch zaufania oraz klucz prywatny, który musi być przechowywany w pliku z rozszerzeniem pfx lub p12. W przypadku nowego certyfikatu należy spełnić wymagania wymienione w poniższej tabeli.

Wymagania dotyczące certyfikatów Serwera administracyjnego

Typ certyfikatu	Wymagania
Certyfikat standardowy, standardowy certyfikat zapasowy („C”, „CR”)	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak Wartość ograniczenia długości ścieżki może być całkowicie inna niż „Brak”, ale nie mniejsza niż „1”. Użycie klucza: • Podpis cyfrowy • Podpisywanie certyfikatów • Szyfrowanie kluczy • Podpisywanie CRL Rozszerzone użycie klucza (EKU): uwierzytelnianie serwera i uwierzytelnianie klienta. Jednostka EKU jest opcjonalna, ale jeśli zawiera ją certyfikat, dane uwierzytelniania serwera i klienta muszą być określone w jednostce EKU.
Certyfikat mobilny, zapasowy certyfikat mobilny („M”, „MR”)	Minimalna długość klucza: 2048. Podstawowe ograniczenia: • Urząd certyfikacji (CA): prawda • Ograniczenie długości ścieżki: brak

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

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

Etapy

Określanie certyfikatu Serwera administracyjnego odbywa się w etapach:

1. **Zastępowanie certyfikatu Serwera administracyjnego**

   W tym celu użyj polecenia narzędzie klsetsrvcert.

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

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

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

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

Wyniki

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

Zastępowanie certyfikatu Serwera administracyjnego za pomocą narzędzia klsetsrvcert

W celu zastąpienia certyfikatu Serwera administracyjnego:

W wierszu polecenia uruchom następujące narzędzie:

```
klsetsrvcert [-t <typ> {-i <plikwejściowy> [-p <hasło>] [-o <chkopt>] | -g <nazwadns>}]
[-f <czas>][-r <calistfile>][-l <plikraportu>]
```

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

Opis parametrów narzędzia klsetsrvcert przedstawia poniższa tabela.

Wartości parametrów narzędzia klsetsrvcert

Parametr	Wartość
`-t <type>`	Typ zastępowanego certyfikatu. Możliwe wartości parametru `<type>` to: • `C` – zastępuje certyfikat standardowy dla portów 13000 i 13291. • `CR` – zastępuje zapasowy certyfikat standardowy dla portów 13000 i 13291. • `M` – zastępuje certyfikat dla urządzeń mobilnych na porcie 13292. • `MR` – zastępuje zapasowy certyfikat mobilny dla portu 13292. • `MCA` – mobilny urząd certyfikacji dla automatycznie wygenerowanych certyfikatów użytkowników.
`-f <time>`	Terminarz zmiany certyfikatu w formacie „DD-MM-RRRR gg:mm" (dla portów: 13000 i 13291).

	Użyj tego parametru, jeśli chcesz zastąpić standardowy lub standardowy certyfikat zapasowy przed jego wygaśnięciem. Określ czas, w którym zarządzane urządzenia muszą synchronizować się z Serwerem administracyjnym na nowym certyfikacie.
`-i <inputfile>`	Kontener z certyfikatem i kluczem prywatnym w formacie PKCS#12 (plik z rozszerzeniem .p12 lub .pfx).
`-p <password>`	Hasło używane do ochrony kontenera p12. Certyfikat i klucz prywatny są przechowywane w kontenerze, dlatego do odszyfrowania pliku z kontenerem wymagane jest hasło.
`-o <chkopt>`	Parametry legalizacji certyfikatu (oddzielone średnikiem). Aby użyć certyfikatu niestandardowego bez uprawnień do podpisywania, określ `-o NoCA` w narzędziu klsetsrvcert. Jest to przydatne w przypadku certyfikatów wydanych przez publiczny urząd certyfikacji.
`-g <dnsname>`	Nowy certyfikat zostanie utworzony dla określonej nazwy DNS.
`-r <calistfile>`	Lista zaufanych urzędów certyfikacji w formacie PEM.
`-l <logfile>`	Zapisuje dane wynikowe. Domyślnie dane wynikowe są przekierowywane do standardowego strumienia wyjściowego.

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

```
klsetsrvcert -t C -i <plikwejściowy> -p <hasło> -o NoCA
```

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

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

```
klsetsrvcert.exe -f "DD-MM-RRRR gg:mm" -t CR -i <plik wejściowy> -p <hasło> -o NoCA
```

gdzie „`DD-MM-RRRR hh:mm`” to data 3–4 tygodnie przed datą bieżącą. Przesunięcie czasowe zmiany certyfikatu na zapasowy pozwoli na rozesłanie nowego certyfikatu do wszystkich Agentów sieciowych.

Podłączanie Agentów sieciowych do Serwera administracyjnego przy użyciu narzędzia klmover

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

W celu określenia nowego certyfikatu Serwera administracyjnego i przywrócenia połączenia:

W wierszu polecenia uruchom następujące narzędzie:

```
klmover [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-
nossl] [-cert <path to certificate file>]
```

Do uruchomienia narzędzia wymagane są uprawnienia administratora.

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

Opis parametrów narzędzia klmover przedstawia poniższa tabela.

Wartości parametrów narzędzia klmover

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

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

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

Ponowne wystawianie certyfikatu serwera sieciowego

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

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

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

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

1. W drzewie konsoli kliknij prawym przyciskiem myszy nazwę odpowiedniego Serwera administracyjnego i z menu kontekstowego wybierz **Właściwości**.
2. W otwartym oknie właściwości Serwera administracyjnego, w lewym panelu wybierz sekcję **Ustawienia połączenia z Serwerem administracyjnym**.
3. Na liście podsekcji wybierz **Certyfikaty**.
4. Jeśli planujesz nadal używać certyfikatu wystawionego przez Kaspersky Security Center, wykonaj następujące czynności:
   a. W prawym okienku, w grupie ustawień **Uwierzytelnianie Serwera administracyjnego przez urządzenia mobilne** wybierz opcję **Certyfikat wydany przez Serwer administracyjny** i kliknij przycisk **Wydaj ponownie**.
   b. W otwartym oknie **Wydaj certyfikat ponownie**, w grupach ustawień **Adres połączenia** i **Czas aktywacji** wybierz odpowiednie opcje i kliknij przycisk **OK**.
   c. W oknie potwierdzenia kliknij przycisk **Tak**.

   Alternatywnie, jeśli planujesz używać własnego certyfikatu niestandardowego, wykonaj następujące czynności:
   a. Sprawdź, czy Twój certyfikat niestandardowy spełnia wymagania Kaspersky Security Center oraz wymagania dotyczące zaufanych certyfikatów firmy Apple. W razie potrzeby zmodyfikuj certyfikat.
   b. Wybierz opcję **Inny certyfikat** i kliknij przycisk **Przeglądaj**.
   c. W otwartym oknie **Certyfikat**, w polu **Typ certyfikatu** wybierz typ swojego certyfikatu, a następnie określ lokalizację i ustawienia certyfikatu:
      - Jeśli został wybrany typ **Kontener PKCS #12**, kliknij przycisk **Przeglądaj** obok pola **Plik certyfikatu** i określ plik certyfikatu na dysku twardym. Jeśli plik certyfikatu jest chroniony hasłem, wprowadź hasło w polu **Hasło (jeśli istnieje)**.
      - Jeśli został wybrany typ **Certyfikat X.509**, kliknij przycisk **Przeglądaj** obok pola **Klucz prywatny (.prk, .pem)** i określ klucz prywatny na dysku twardym. Jeśli klucz prywatny jest chroniony hasłem, wprowadź hasło w polu **Hasło (jeśli istnieje)**. Następnie kliknij przycisk **Przeglądaj** obok pola **Klucz publiczny (.cer)** i określ klucz prywatny na dysku twardym.
   d. W oknie **Certyfikat** kliknij **OK**.
   e. W oknie potwierdzenia kliknij przycisk **Tak**.

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

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

1. Wygeneruj swój certyfikat niestandardowy i przygotuj go do użycia w Kaspersky Security Center. Sprawdź, czy Twój certyfikat niestandardowy spełnia wymagania Kaspersky Security Center oraz wymagania dotyczące zaufanych certyfikatów firmy Apple. W razie potrzeby zmodyfikuj certyfikat.

   Możesz użyć narzędzia kliossrvcertgen.exe do generowania certyfikatu.

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

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

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

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

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

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

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

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

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

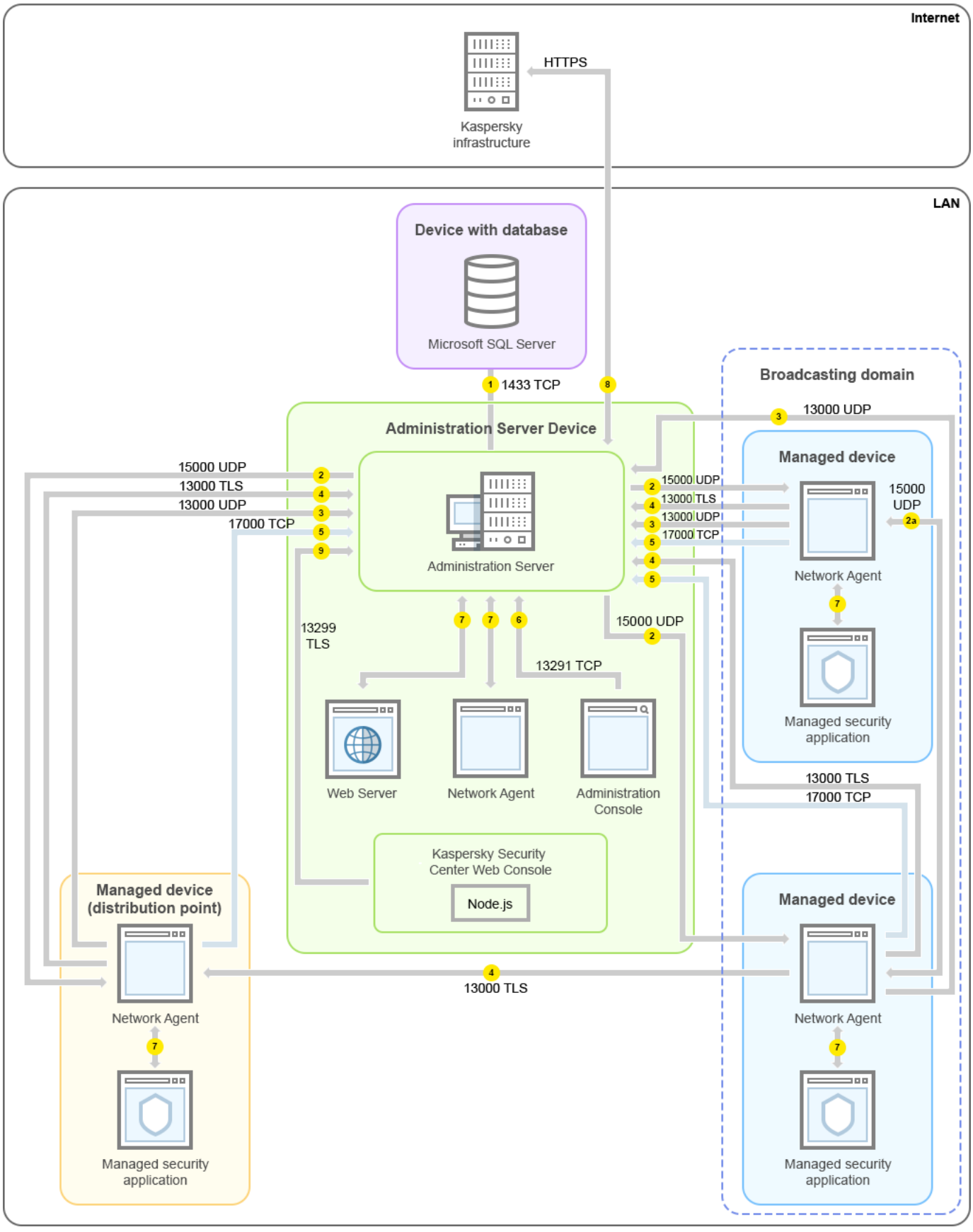
   Certyfikat serwera sieciowego został ponownie wystawiony.

Schematy ruchu sieciowego danych i użycia portów

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

Serwer administracyjny i zarządzane urządzenia w sieci LAN

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



Serwer administracyjny i zarządzane urządzenia w sieci lokalnej (LAN)

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

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

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

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

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

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

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

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

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

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

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

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

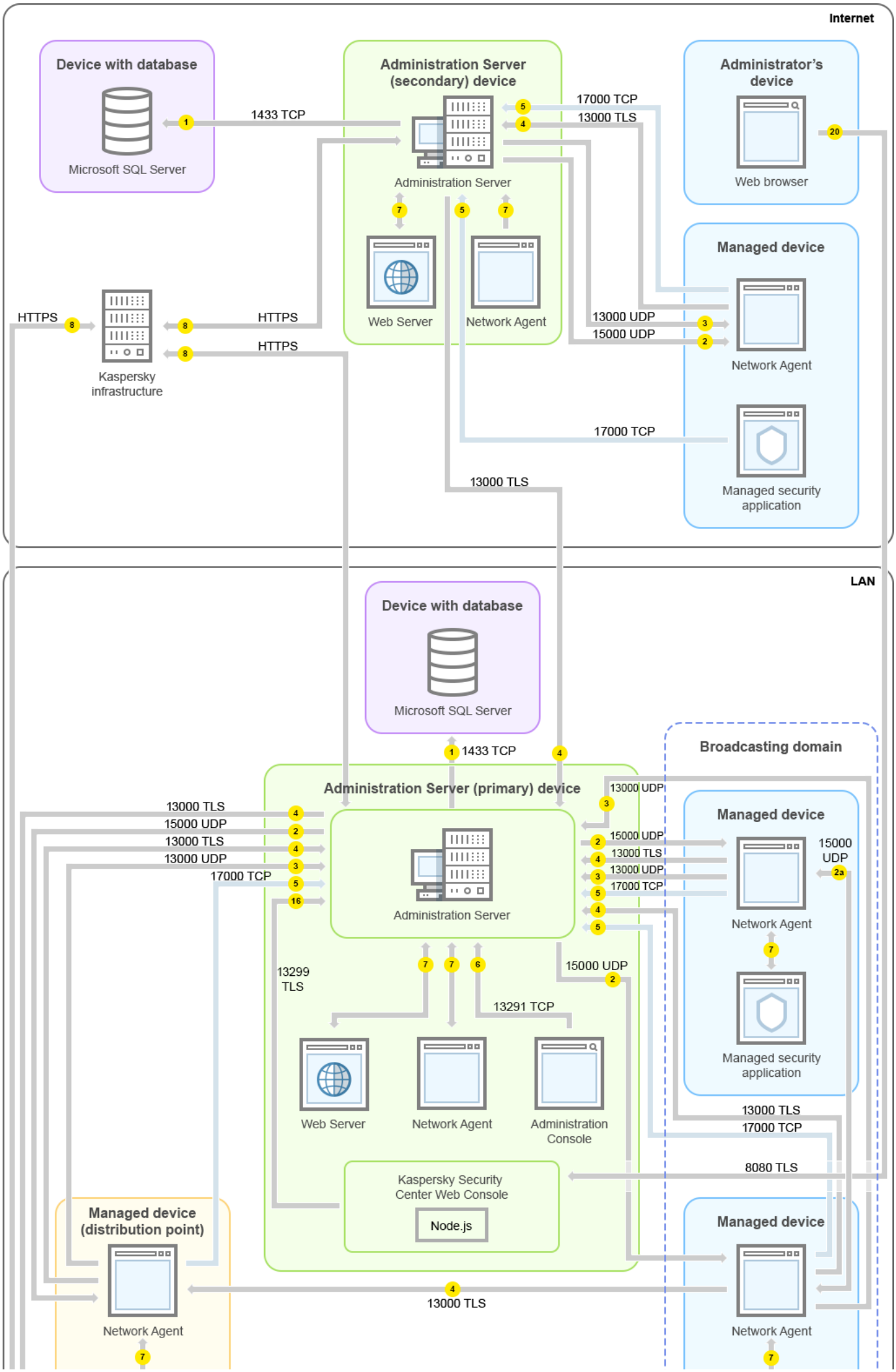
8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

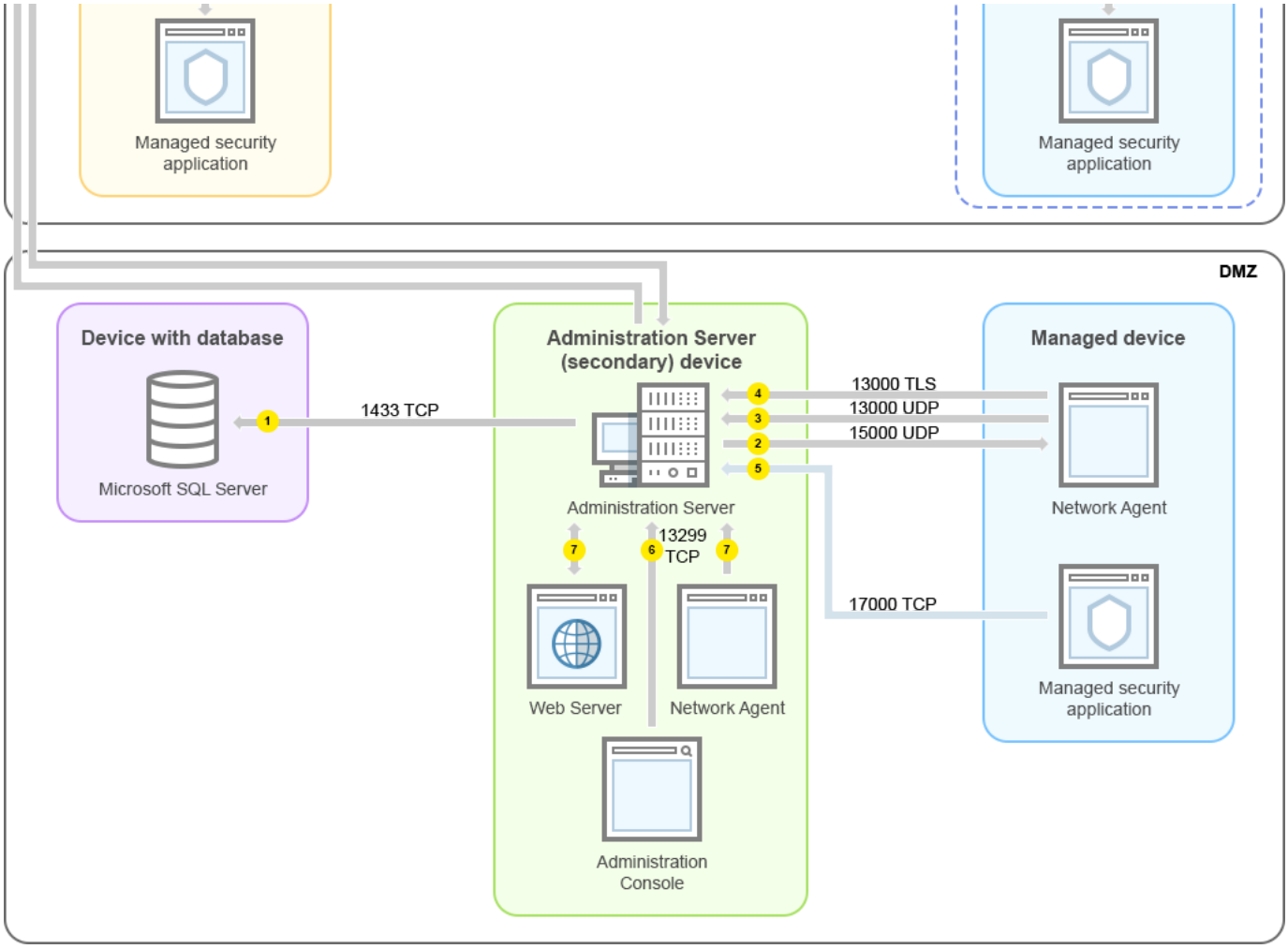
   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do Internetu, musisz ręcznie zarządzać tymi danymi.

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

Główny Serwer administracyjny w sieci LAN i dwa podrzędne Serwery administracyjne

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


Internet
Device with database
Microsoft SQL Server
1433 TCP
Administration Server (secondary) device
Administration Server
Web Server
Network Agent
17000 TCP
13000 TLS
Administrator's device
Web browser
Managed device
Network Agent
13000 UDP
15000 UDP
17000 TCP
Managed security application
13000 TLS
HTTPS
Kaspersky infrastructure
LAN
Device with database
Microsoft SQL Server
1433 TCP
Broadcasting domain
Administration Server (primary) device
Administration Server
13000 TLS
15000 UDP
13000 TLS
13000 UDP
17000 TCP
Managed device
Network Agent
15000 UDP
Managed security application
13299 TLS
13291 TCP
Web Server
Network Agent
Administration Console
Kaspersky Security Center Web Console
Node.js
8080 TLS
Managed device (distribution point)
Network Agent
13000 TLS



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

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

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

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

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

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

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

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

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

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

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

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

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

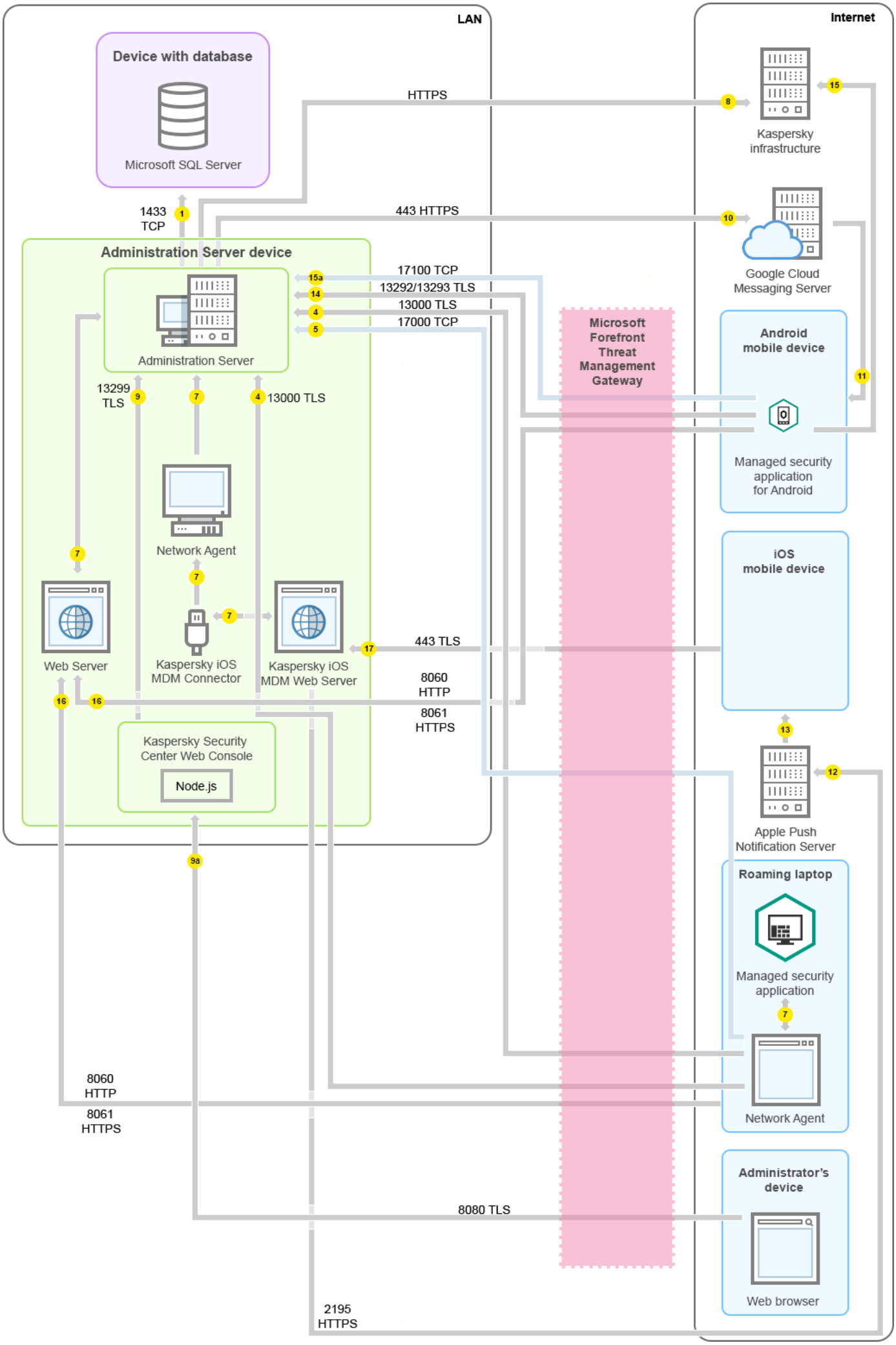
   Jeśli nie chcesz, żeby Twój Serwer administracyjny miał dostęp do Internetu, musisz ręcznie zarządzać tymi danymi.

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

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

Serwer administracyjny w sieci LAN, zarządzane urządzenia w Internecie, TMG w użyciu

Poniższy rysunek przedstawia ruch sieciowy danych, gdy Serwer administracyjny jest w sieci lokalnej (LAN), a zarządzane urządzenia, w tym urządzenia mobilne, są w internecie. Na tym rysunku *Microsoft Forefront Threat Management Gateway* (TMG) jest w użyciu. Jednakże, jeśli chcesz używać firmowej zapory sieciowej, możesz użyć innej aplikacji; więcej informacji znajdziesz w dokumentacji dla wybranej aplikacji.


LAN
Internet
Device with database
Microsoft SQL Server
HTTPS
Kaspersky infrastructure
1433 TCP
443 HTTPS
Google Cloud Messaging Server
Administration Server device
17100 TCP
13292/13293 TLS
13000 TLS
17000 TCP
Administration Server
Microsoft Forefront Threat Management Gateway
Android mobile device
13299 TLS
13000 TLS
Managed security application for Android
Network Agent
iOS mobile device
Web Server
Kaspersky iOS MDM Connector
Kaspersky iOS MDM Web Server
443 TLS
8060 HTTP
8061 HTTPS
Kaspersky Security Center Web Console
Node.js
Apple Push Notification Server
Roaming laptop
Managed security application
8060 HTTP
8061 HTTPS
Network Agent
Administrator's device
8080 TLS
Web browser
2195 HTTPS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14. Tylko dla urządzeń mobilnych: dane z zarządzanej aplikacji są przesyłane do Serwera administracyjnego (lub do bramy połączenia) poprzez port TLS o numerze 13292 / 13293— bezpośrednio lub poprzez Microsoft Forefront Threat Management Gateway (TMG).

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

    15a. Jeśli urządzenie mobilne nie ma dostępu do Internetu, dane są przesyłane do Serwera administracyjnego poprzez port o numerze 17100, a Serwer administracyjny wysyła je do infrastruktury Kaspersky; jednakże ten scenariusz jest stosowany bardzo rzadko.

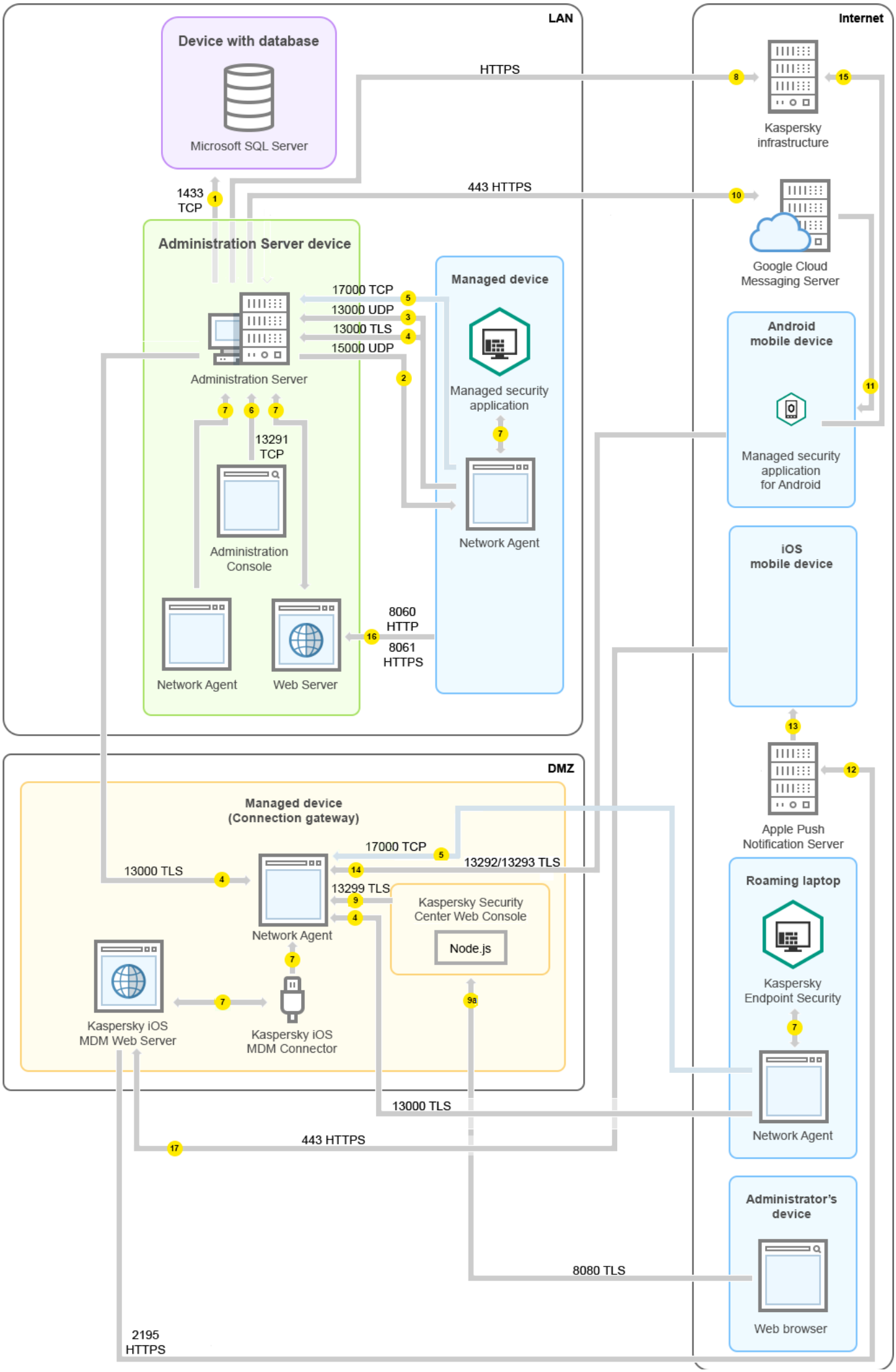
16. Żądania dla pakietów z zarządzanych urządzeń, w tym urządzeń mobilnych, są przesyłane do serwera WWW, który znajduje się na tym samym urządzeniu co Serwer administracyjny.

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

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

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

Ten schemat wdrażania jest zalecany, jeśli nie chcesz, żeby urządzenia mobilne nawiązywały połączenie bezpośrednio z Serwerem administracyjnym i nie chcesz używać Microsoft Forefront Threat Management Gateway (TMG) lub firmowej zapory sieciowej.


LAN
Internet
Device with database
Microsoft SQL Server
HTTPS
Kaspersky infrastructure
1433 TCP
443 HTTPS
Google Cloud Messaging Server
Administration Server device
Managed device
17000 TCP
13000 UDP
13000 TLS
15000 UDP
Administration Server
Managed security application
Android mobile device
Managed security application for Android
13291 TCP
Administration Console
Network Agent
iOS mobile device
8060 HTTP
8061 HTTPS
Network Agent
Web Server
DMZ
Managed device (Connection gateway)
17000 TCP
13292/13293 TLS
13000 TLS
13299 TLS
Kaspersky Security Center Web Console
Node.js
Network Agent
Apple Push Notification Server
Roaming laptop
Kaspersky Endpoint Security
Kaspersky iOS MDM Web Server
Kaspersky iOS MDM Connector
13000 TLS
Network Agent
443 HTTPS
Administrator's device
8080 TLS
Web browser
2195 HTTPS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14. Tylko dla urządzeń mobilnych: dane z zarządzanej aplikacji są przesyłane do Serwera administracyjnego (lub do bramy połączenia) poprzez port TLS o numerze 13292 / 13293— bezpośrednio lub poprzez Microsoft Forefront Threat Management Gateway (TMG).

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

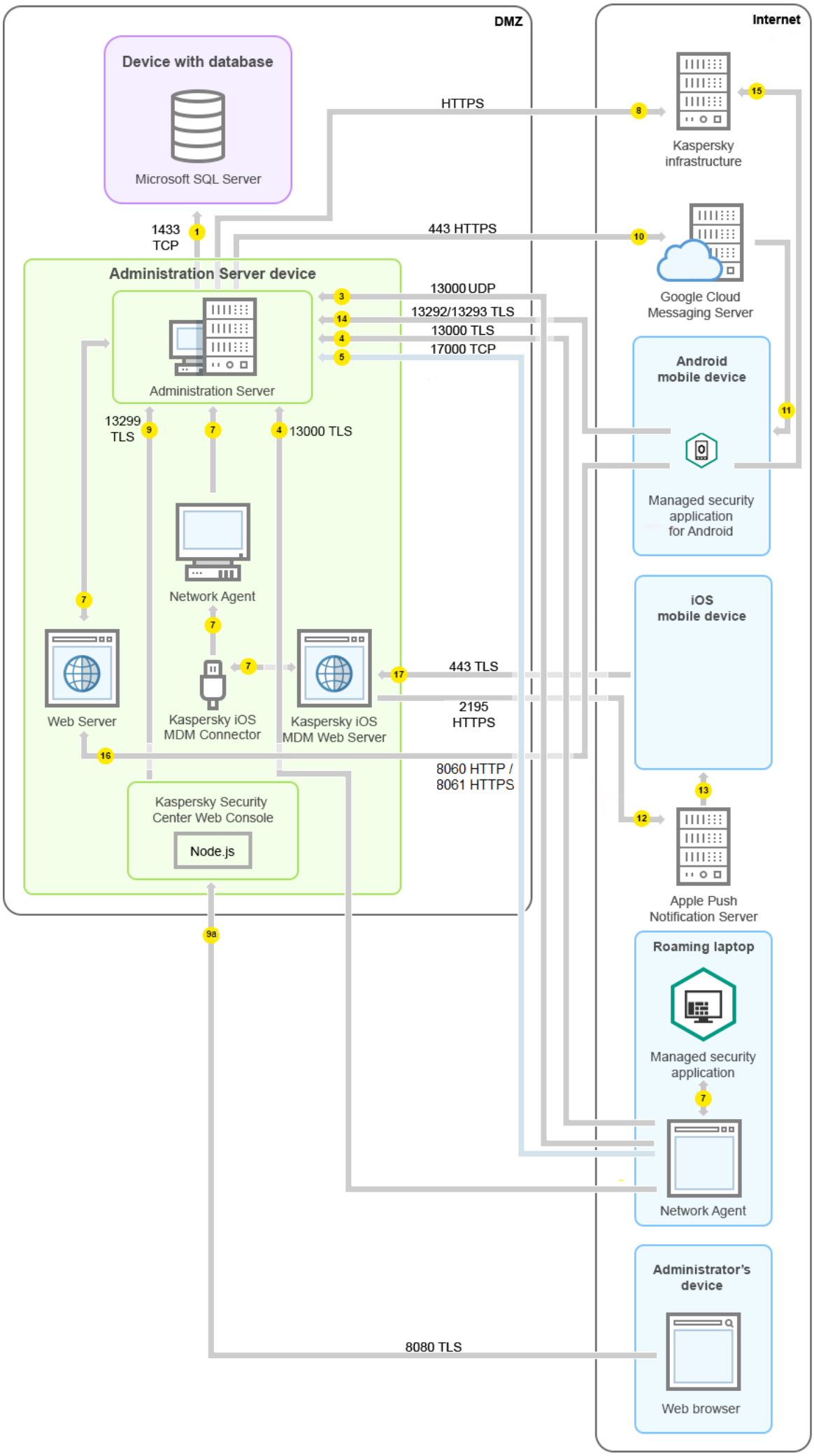
    15a. Jeśli urządzenie mobilne nie ma dostępu do Internetu, dane są przesyłane do Serwera administracyjnego poprzez port o numerze 17100, a Serwer administracyjny wysyła je do infrastruktury Kaspersky; jednakże ten scenariusz jest stosowany bardzo rzadko.

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

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

Serwer administracyjny w strefie DMZ, zarządzane urządzenia w Internecie

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


DMZ
Internet
Device with database
Microsoft SQL Server
HTTPS
8
15
Kaspersky infrastructure
1433 TCP
1
443 HTTPS
10
Google Cloud Messaging Server
Administration Server device
3
13000 UDP
14
13292/13293 TLS
4
13000 TLS
5
17000 TCP
Administration Server
Android mobile device
11
13299 TLS
9
7
4
13000 TLS
Managed security application for Android
Network Agent
7
iOS mobile device
Web Server
Kaspersky iOS MDM Connector
Kaspersky iOS MDM Web Server
17
443 TLS
2195 HTTPS
16
8060 HTTP / 8061 HTTPS
13
12
Apple Push Notification Server
Kaspersky Security Center Web Console
Node.js
9a
Roaming laptop
Managed security application
Network Agent
Administrator's device
8080 TLS
Web browser

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

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

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

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

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

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

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

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

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

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

   Urządzenia mobilne nawiązują także połączenie z bramą połączenia za pośrednictwem portu SSL o numerze 13000.

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

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

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

8. Dane z Serwera administracyjnego na serwery Kaspersky (takie jak dane KSN lub informacje o licencjach) oraz dane z serwerów Kaspersky na Serwer administracyjny (takie jak uaktualnienia aplikacji i aktualizacje

antywirusowych baz danych) są przesyłane przy użyciu protokołu HTTPS.

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

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

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

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

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

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

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

14. Tylko dla urządzeń mobilnych: dane z zarządzanej aplikacji są przesyłane do Serwera administracyjnego (lub do bramy połączenia) poprzez port TLS o numerze 13292 / 13293— bezpośrednio lub poprzez Microsoft Forefront Threat Management Gateway (TMG).

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

    15a. Jeśli urządzenie mobilne nie ma dostępu do Internetu, dane są przesyłane do Serwera administracyjnego poprzez port o numerze 17100, a Serwer administracyjny wysyła je do infrastruktury Kaspersky; jednakże ten scenariusz jest stosowany bardzo rzadko.

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

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

Interakcja komponentów Kaspersky Security Center i aplikacji zabezpieczających: więcej informacji

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

Konwencje stosowane w schematach interakcji

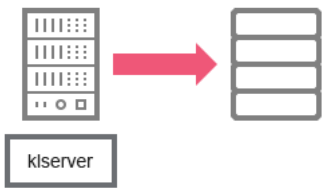
Poniższa tabela przedstawia konwencje stosowane w schematach.

Oznaczenia stosowane w dokumencie

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

Serwer administracyjny i DBMS

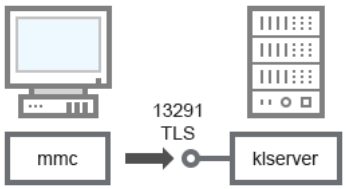
Dane z Serwera administracyjnego wprowadź w bazie danych serwera SQL, MySQL lub MariaDB.



Serwer administracyjny i DBMS

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

Serwer administracyjny i Konsola administracyjna



Serwer administracyjny i Konsola administracyjna

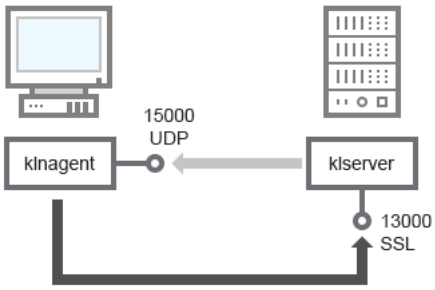
Klasyfikacje schematu są dostępne w tabeli poniżej.

Serwer administracyjny i Konsola administracyjna (ruch sieciowy)

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

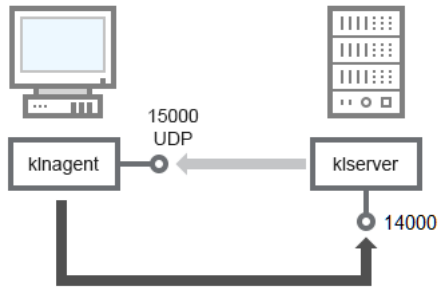
Serwer administracyjny i urządzenie klienckie: zarządzanie aplikacją zabezpieczająca

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



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

Jeśli używałeś wcześniejszej wersji Kaspersky Security Center, Serwer administracyjny w Twojej sieci może odbierać połączenia od Agentów sieciowych poprzez port bez szyfrowania SSL o numerze 14000 (patrz rysunek poniżej). Kaspersky Security Center 14.2 obsługuje także połączenia Agentów sieciowych poprzez port 14000, chociaż zalecane jest korzystanie z portu SSL o numerze 13000.



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

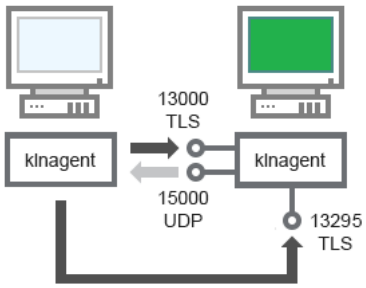
Wyjaśnienie schematów jest dostępne w tabeli poniżej.

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

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

Aktualizowanie oprogramowania na urządzeniu klienckim poprzez punkt dystrybucji

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



Aktualizowanie oprogramowania na urządzeniu klienckim poprzez punkt dystrybucji

Klasyfikacje schematu są dostępne w tabeli poniżej.

Aktualizowanie oprogramowania za pośrednictwem punktu dystrybucji (ruch sieciowy)

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

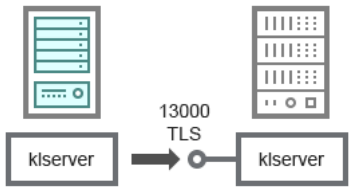
Punkt dystrybucji	13295	klnagent	TCP	Tak	Wysyłanie powiadomień typu push do Agenta sieciowego

Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i podrzędny Serwer administracyjny

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

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

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



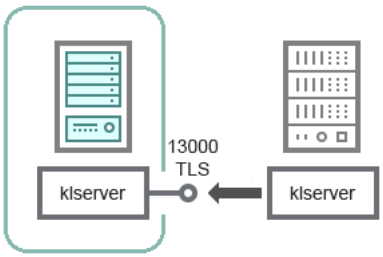
Hierarchia Serwerów administracyjnych: główny Serwer administracyjny i podrzędny Serwer administracyjny

Klasyfikacje schematu są dostępne w tabeli poniżej.

Hierarchia Serwerów administracyjnych (ruch sieciowy)

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

Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ



Hierarchia Serwerów administracyjnych z podrzędnym Serwerem administracyjnym w strefie DMZ

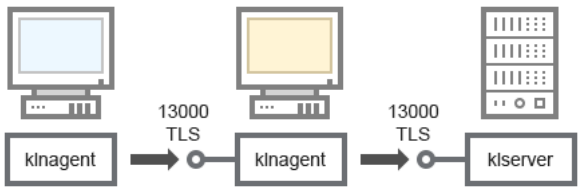
Schemat przedstawia hierarchię Serwerów administracyjnych, w której podrzędny Serwer administracyjny, znajdujący się w strefie DMZ, odbiera połączenie z głównego Serwera administracyjnego (patrz tabela poniżej dla wyjaśnienia schematu). Podczas łączenia dwóch Serwerów administracyjnych w hierarchię upewnij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

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

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

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

Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie



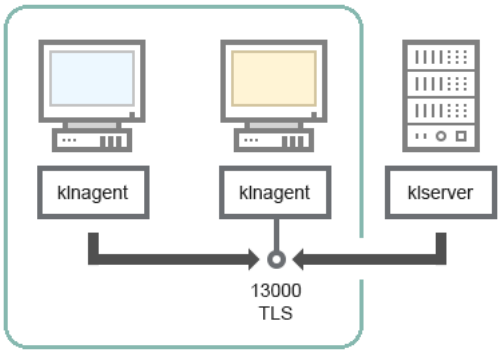
Serwer administracyjny, brama połączenia w segmencie sieci i urządzenie klienckie

Klasyfikacje schematu są dostępne w tabeli poniżej.

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

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

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



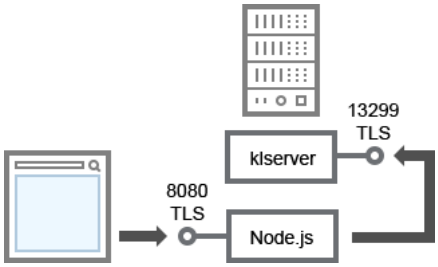
Serwer administracyjny z bramą połączenia i urządzeniem klienckim w strefie DMZ

Klasyfikacje schematu są dostępne w tabeli poniżej.

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

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

Serwer administracyjny i Kaspersky Security Center Web Console



Serwer administracyjny i Kaspersky Security Center Web Console

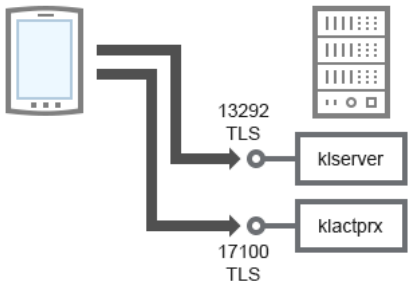
Klasyfikacje schematu są dostępne w tabeli poniżej.

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

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

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

Aktywowanie i zarządzanie aplikacją zabezpieczającą na urządzeniu mobilnym



Aktywowanie i zarządzanie aplikacją zabezpieczającą na urządzeniu mobilnym

Klasyfikacje schematu są dostępne w tabeli poniżej.

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

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

Wdrażanie praktycznego zastosowania aplikacji

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

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

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

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

Przewodnik zwiększania bezpieczeństwa

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

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

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

Przewodnik zwiększania bezpieczeństwa zawiera następujące informacje:

- Wybór architektury Serwera administracyjnego
- Konfigurowanie bezpiecznego połączenia z Serwerem administracyjnym
- Konfigurowanie kont w celu uzyskania dostępu do Serwera administracyjnego
- Zarządzanie ochroną Serwera administracyjnego
- Zarządzanie ochroną urządzeń klienckich
- Konfigurowanie ochrony dla zarządzanych aplikacji
- Konserwacja Serwera administracyjnego
- Przesyłanie informacji do aplikacji firm trzecich

Wdrożenie Serwera administracyjnego

Architektura Serwera administracyjnego

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

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

Na podstawie tych informacji można utworzyć architekturę, która określa:

- Lokalizacja Serwera administracyjnego i połączenia sieciowe
- Organizacja obszarów roboczych administratora i metody łączenia się z Serwerem administracyjnym
- Metody instalacji agenta sieciowego i oprogramowania zabezpieczającego

- Korzystanie z punktów dystrybucji
- Korzystanie z wirtualnych Serwerów administracyjnych
- Użycie hierarchii Serwerów administracyjnych
- Schemat aktualizacji antywirusowej bazy danych
- Inne przepływy informacji

Wybieranie urządzenia do instalacji Serwera administracyjnego

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

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

Lokalizacja Serwera administracyjnego

Urządzenia zarządzane przez Serwer administracyjny można zlokalizować w następujący sposób:

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

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

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

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

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

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

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

Konta do instalowania i uruchamiania Serwera administracyjnego

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

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

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

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

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

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

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

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

Wykluczanie Serwera administracyjnego z domeny

Nie zalecamy dołączania urządzenia Serwera administracyjnego do domeny (jeśli jest używana). Pozwala to rozróżnić uprawnienia zarządzania Kaspersky Security Center i uniemożliwić dostęp do Serwera administracyjnego w przypadku naruszenia bezpieczeństwa konta domeny.

Bezpieczeństwo połączenia

Użycie TLS

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

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

Ścisłe ustawienia TLS

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

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

Ograniczanie dostępu do bazy danych Serwera administracyjnego

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

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

Zakaz zdalnego uwierzytelniania przy użyciu kont Windows

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

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

1. Użyj narzędzia klscflag, aby określić wartość flagi LP_RestrictRemoteOsAuth:

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

2. Uruchom ponownie usługę Serwera administracyjnego.

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

Autoryzacja Microsoft SQL Server

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

Konfigurowanie listy dozwolonych adresów IP do łączenia się z Serwerem administracyjnym

Domyślnie użytkownicy mogą logować się do Kaspersky Security Center z dowolnego urządzenia, na którym mogą otworzyć Kaspersky Security Center Web Console lub na którym zainstalowana jest Konsola administracyjna oparta na MMC. Możesz jednak skonfigurować Serwer administracyjny tak, aby użytkownicy mogli łączyć się z nim tylko z urządzeń o dozwolonych adresach IP. W takim przypadku, nawet jeśli intruz ukradnie konto Kaspersky Security Center, będzie mógł zalogować się do Kaspersky Security Center tylko z adresów IP znajdujących się na liście dozwolonych.

Konta i uwierzytelnianie

Używanie weryfikacji dwuetapowej z Serwerem administracyjnym

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

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

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

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

Używanie uwierzytelniania dwuskładnikowego dla systemu operacyjnego

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

Zakaz zapisywania hasła administratora

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

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

Uwierzytelnianie wewnętrznego konta użytkownika

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

- Hasło musi zawierać od 8 do 16 znaków.
- Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
  - Wielkie litery (A-Z)

- Małe litery (a-z)
- Cyfry (0-9)
- Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

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

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

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

Dedykowana grupa administracyjna dla Serwera administracyjnego

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

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

Grupy KLAdmins i KLOperators

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

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

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

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

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

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

Ograniczanie członkostwa w roli Głównego administratora

Zalecamy ograniczenie członkostwa w roli Głównego administratora.

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

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

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

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

Zakaz uwierzytelniania przy użyciu kont Windows

Gdy urządzenie Serwera administracyjnego zostanie przejęte, niezaufane konta mogą zostać dodane do grupy KLAdmins, uzyskując w ten sposób dostęp do Serwera administracyjnego i możliwości administratora.

Możesz zablokować uwierzytelnianie na Serwerze administracyjnym przy użyciu kont Windows.

W tym celu dodaj w ustawieniach zabezpieczeń wbudowaną grupę Wszyscy oraz Użytkownicy domeny, a następnie zablokuj wszystkie operacje dla tych grup (opcjonalnie możesz pozostawić prawa do odczytu).
Grupa Wszyscy obejmuje wszystkich użytkowników, nawet użytkowników anonimowych i gości. Członkostwo w grupie jest kontrolowane przez system operacyjny.

Jeśli zastosujesz te ustawienia, uwierzytelnianie na Serwerze administracyjnym będzie możliwe tylko dla użytkowników wewnętrznych. Przed zastosowaniem ustawień upewnij się, że co najmniej jeden użytkownik wewnętrzny został utworzony i ma przypisaną rolę głównego administratora. Jeśli bieżący użytkownik utraci dostęp do Serwera administracyjnego po zastosowaniu ustawień, Serwer administracyjny wyśle o tym powiadomienie.

Nawet jeśli użytkownik należy do grupy KLAdmins, użytkownik nie uzyska dostępu do Serwera administracyjnego, ponieważ reguły blokowania mają wyższy priorytet niż reguły zezwalające.

Przed użyciem tego ustawienia upewnij się, że utworzono wewnętrzne konta administratora. Nieprawidłowe użycie tego ustawienia może doprowadzić do utraty kontroli nad Serwerem administracyjnym.

Konfigurowanie praw dostępu do funkcji aplikacji

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

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

Główne zalety modelu kontroli dostępu opartego na rolach:

- Łatwość administracji

- Hierarchia ról
- Podejście w oparciu o najmniejsze uprawnienia
- Podział obowiązków

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

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

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

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

Osobne konto do zdalnej instalacji aplikacji

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

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

Zabezpieczanie uprzywilejowanego dostępu do systemu Windows

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

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

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

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

Regularny audyt wszystkich użytkowników

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

Zarządzanie ochroną Serwera administracyjnego

Wybieranie oprogramowania zabezpieczającego Serwer administracyjny

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

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

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

- Kaspersky Industrial CyberSecurity for Nodes. Zalecamy zainstalowanie tej aplikacji na urządzeniach wchodzących w skład sieci przemysłowej. Kaspersky Industrial CyberSecurity for Nodes to aplikacja, która posiada certyfikaty kompatybilności z różnymi producentami oprogramowania przemysłowego.

- Zalecane produkty zabezpieczające. Jeśli Serwer administracyjny jest zainstalowany na urządzeniu z innym oprogramowaniem, zalecamy wzięcie pod uwagę zaleceń tego dostawcy oprogramowania dotyczących kompatybilności produktów zabezpieczających (mogą już istnieć zalecenia dotyczące wyboru rozwiązania zabezpieczającego i konieczne może być skonfigurowanie strefy zaufanej).

Tworzenie osobnej polityki bezpieczeństwa dla aplikacji zabezpieczającej

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

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

Moduły ochrony

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

Konfigurowanie zapory sieciowej urządzenia Serwera administracyjnego

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

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

Zakaz uruchamiania panelu sterowania

Jeśli instalujesz Serwer administracyjny na urządzeniu z systemem Microsoft Windows i używasz aplikacji ochronnej z modułem Kontrola uruchamiania aplikacji, możesz zabronić uruchamiania panelu sterowania (control.exe) użytkownikom nieuprzywilejowanym, na przykład grupie Administratorzy.

Po utworzeniu określonych reguł kontrolujących uruchamianie aplikacji, użytkownicy z uprawnieniami predefiniowanej roli Administratora tracą możliwość kontrolowania innych kont sieciowych, w tym zmiany swoich loginów i haseł.

Zarządzanie ochroną urządzeń klienckich

Ograniczenie dodawania kluczy licencyjnych do pakietów instalacyjnych

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

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

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

Automatyczne reguły przenoszenia urządzeń pomiędzy grupami administracyjnymi

Zalecamy ograniczenie stosowania automatycznych reguł przenoszenia urządzeń między grupami administracyjnymi.

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

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

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

Wymagania bezpieczeństwa dla punktów dystrybucji i bram połączeń

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

- Rozsyłaj aktualizacje i pakiety instalacyjne otrzymane z Serwera administracyjnego na urządzenia klienckie w grupie.

- Wykonaj zdalną instalację oprogramowania innych firm i aplikacji Kaspersky na urządzeniach klienckich.
- Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może wykorzystywać te same metody wykrywania urządzeń, co Serwer administracyjny.

Umieszczanie punktów dystrybucji w sieci organizacji służących do:

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

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

Ograniczenie automatycznego przydzielania punktów dystrybucji

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

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

Możesz także przeglądać Raport z działalności punktów dystrybucji.

Konfigurowanie ochrony dla zarządzanych aplikacji

Zasady aplikacji zarządzanych

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

Określenie hasła do wyłączenia ochrony i odinstalowania aplikacji

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

Używanie Kaspersky Security Network

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

Regularne skanowanie zarządzanych urządzeń

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

Odkrywanie nowych urządzeń

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

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

Wybieranie folderu współdzielonego

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

Konserwacja Serwera administracyjnego

Tworzenie kopii zapasowych danych Serwera administracyjnego

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

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

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

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

Konserwacja Serwera administracyjnego

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

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

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

Instalowanie aktualizacji systemu operacyjnego i aktualizacji oprogramowania innych firm

Zdecydowanie zalecamy regularne instalowanie aktualizacji oprogramowania dla systemu operacyjnego i oprogramowania innych firm na urządzeniu Serwera administracyjnego.

Urządzenia klienckie nie wymagają ciągłego połączenia z Serwerem administracyjnym, dlatego bezpieczne jest ponowne uruchomienie urządzenia Serwera administracyjnego po zainstalowaniu aktualizacji. Wszystkie zdarzenia zarejestrowane na urządzeniach klienckich podczas przestoju Serwera administracyjnego są do niego wysyłane po przywróceniu połączenia.

Transfer zdarzeń do systemów innych producentów

Monitorowanie i raportowanie

W celu szybkiego reagowania na incydenty związane z bezpieczeństwem zalecamy skonfigurowanie funkcji monitorowania i raportowania.

Eksportowanie zdarzeń do systemów SIEM

W celu szybkiego wykrycia incydentów, zanim wystąpią poważne szkody, zalecamy wykorzystanie eksportu zdarzeń w systemie SIEM.

Powiadomienia e-mail o zdarzeniach audytu

Kaspersky Security Center umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. W celu szybkiego reagowania na sytuacje awaryjne zalecamy skonfigurowanie Serwera administracyjnego do wysyłania powiadomień o zdarzeniach audytu, zdarzeniach krytycznych, zdarzeniach błędu i ostrzeżeniach, które publikuje.

Ponieważ zdarzenia te są zdarzeniami wewnątrzsystemowymi, można spodziewać się ich niewielkiej liczby, co ma zastosowanie w przypadku wysyłki.

Przygotowanie do zdalnej instalacji

Ta sekcja opisuje kroki, jakie należy podjąć przed zainstalowaniem Kaspersky Security Center.

Planowanie instalacji Kaspersky Security Center

Ta sekcja zawiera informacje o najbardziej odpowiednich opcjach instalacji komponentów Kaspersky Security Center w sieci organizacji w zależności od następujących kryteriów:

- Całkowitą liczbę urządzeń.
- Jednostki (biura lokalne, oddziały), które są oddalone geograficznie lub pod względem organizacyjnym
- Oddalone od siebie sieci połączone wąskimi kanałami
- Potrzeba uzyskania dostępu do Serwera administracyjnego przez Internet

Typowe schematy wdrażania systemu ochrony

Ta sekcja opisuje standardowe schematy wdrażania systemu ochrony w sieci firmowej, korzystając z Kaspersky Security Center.

System musi być chroniony przed wszelkimi rodzajami nieautoryzowanego dostępu. Przed zainstalowaniem aplikacji na urządzeniu i fizyczną ochroną Serwerów administracyjnych i punktów dystrybucji zalecamy zainstalowanie wszystkich dostępnych aktualizacji zabezpieczeń dla systemu operacyjnego.

Możesz użyć Kaspersky Security Center do wdrożenia systemu ochrony w sieci korporacyjnej, wykorzystując następujące schematy:

- Wdrożenie systemu ochrony poprzez Kaspersky Security Center przy pomocy jednej z następujących metod:
  - Poprzez Konsolę administracyjną
  - Poprzez Kaspersky Security Center Web Console

  Aplikacje Kaspersky są instalowane automatycznie na urządzeniach klienckich, które łączą się automatycznie z Serwerem administracyjnym poprzez Kaspersky Security Center.

  Podstawowy schemat zdalnej instalacji to instalacja systemu ochrony poprzez Konsolę administracyjną. Korzystanie z Kaspersky Security Center Web Console umożliwia instalację aplikacji Kaspersky z poziomu przeglądarki internetowej.
- Ręczna instalacja systemu ochrony przy pomocy autonomicznych pakietów instalacyjnych wygenerowanych przez Kaspersky Security Center.

  Instalacja aplikacji Kaspersky na urządzeniach klienckich i stacji roboczej administratora jest wykonywana ręcznie; ustawienia połączenia urządzeń klienckich z Serwerem administracyjnym są określane podczas instalacji Agenta sieciowego.

  Ta metoda instalacji jest zalecana w sytuacjach, gdy zdalna instalacja nie jest możliwa.

Kaspersky Security Center umożliwia także wdrożenie systemu ochrony przy użyciu zasad grupy Microsoft Active Directory®.

Informacje dotyczące planowania instalacji Kaspersky Security Center w sieci organizacji

Jeden Serwer administracyjny może obsługiwać maksymalnie 100 000 urządzeń. Jeśli całkowita liczba urządzeń w sieci organizacji przekroczy 100 000, wówczas w tej sieci należy zainstalować kilka Serwerów administracyjnych i połączyć je w hierarchię w celu uproszczenia scentralizowanego zarządzania.

Jeśli organizacja zawiera znaczną liczbę zdalnych biur lokalnych (oddziałów), z których każdy posiada swojego administratora, znacznym ułatwieniem będzie zainstalowanie Serwera administracyjnego w każdym z tych biur. W przeciwnym razie biura te należy postrzegać jako odizolowane sieci komunikujące się przez wąskie kanały (patrz sekcja „Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów").

Podczas korzystania z oddalonych od siebie sieci połączonych wąskimi kanałami, ruch sieciowy można zmniejszyć, wskazując kilku Agentów sieciowych jako punkty dystrybucji (zapoznaj się z tabelą zawierającą wyliczenie liczby punktów dystrybucji). W tym przypadku wszystkie urządzenia w oddalonej sieci pobierają uaktualnienia z tych lokalnych centrów aktualizacji. Punkty dystrybucji mogą pobrać uaktualnienia zarówno z Serwera administracyjnego (domyślny scenariusz) oraz z serwerów Kaspersky dostępnych w Internecie (patrz sekcja „Standardowa konfiguracja: Małe zdalne biura").

Sekcja „Standardowa konfiguracja Kaspersky Security Center" zawiera szczegółowy opis standardowej konfiguracji Kaspersky Security Center. Podczas planowania instalacji wybierz najodpowiedniejszą konfigurację, mając na uwadze strukturę organizacji.

Na etapie planowania instalacji należy rozważyć przydzielenie do Serwera administracyjnego specjalnego certyfikatu X.509. Przydzielenie certyfikatu X.509 do Serwera administracyjnego może być przydatne między innymi do:

- Sprawdzania ruchu SSL poprzez kończenie żądań SSL na serwerze proxy lub do korzystania ze zwrotnego serwera proxy
- Integracji z infrastrukturą kluczy publicznych (PKI) organizacji
- Określenia wymaganych wartości w polach certyfikatu
- Zapewnienia wymaganej siły szyfrowania certyfikatu

Wybieranie struktury ochrony firmy

Wybór struktury ochrony organizacji jest definiowany przez następujące czynniki:

- Topologię sieci firmy.
- Strukturę organizacyjną.
- Liczbę pracowników zajmujących się ochroną sieci, a także zakres ich obowiązków.
- Zasoby sprzętu, które mogą zostać przydzielone dla komponentów do zarządzania ochroną.
- Przepustowość kanałów komunikacji, które mogą zostać przydzielone w celu utrzymania działania składników ochrony w sieci organizacji.
- Ograniczenia czasu wykonywania krytycznych działań administracyjnych w sieci firmowej. Na krytyczne działania administracyjne składają się, na przykład, dystrybucja uaktualnień antywirusowych baz danych i modyfikacja profili dla urządzeń klienckich.

Podczas wybierania struktury ochrony zalecamy najpierw określić dostępną sieć i zasoby sprzętu, które będą wykorzystane do działania scentralizowanego systemu ochrony.

W celu przeprowadzenia analizy infrastruktury sprzętu i sieci zalecane jest wykonanie następujących czynności:

1. Określenie następujących ustawień sieci, w obrębie której zostanie zainstalowana ochrona:
   - Liczba segmentów sieci.
   - Prędkość komunikacji przez kanały komunikacyjne pomiędzy pojedynczymi segmentami sieci.
   - Liczba zarządzanych urządzeń w każdym segmencie sieci.
   - Przepustowość każdego kanału komunikacji, który może zostać przydzielony w celu utrzymania działania ochrony.
2. Określenie maksymalnego dozwolonego czasu na wykonanie kluczowych działań administracyjnych dla wszystkich zarządzanych urządzeń.
3. Przeanalizuj informacje z kroków 1 i 2, a także dane z testów obciążeniowych systemu administracyjnego. Opierając się na wynikach analizy, odpowiedz na następujące pytania:
   - Czy jest możliwa obsługa wszystkich klientów przy pomocy pojedynczego Serwera administracyjnego, czy też niezbędna jest hierarchia Serwerów administracyjnych?
   - Jaka konfiguracja sprzętowa Serwerów administracyjnych jest potrzebna do zajmowania się wszystkimi klientami w przedziale czasu określonym w punkcie 2?
   - Czy konieczne jest użycie punktów dystrybucji do zmniejszenia obciążenia kanałów komunikacji?

Po uzyskaniu odpowiedzi na powyższe pytania, możesz stworzyć zestaw dozwolonych struktur ochrony organizacji.

W sieci firmowej można użyć jednej z poniższych standardowych struktur ochrony:

- Jeden Serwer administracyjny. Wszystkie urządzenia klienckie są połączone z jednym Serwerem administracyjnym. Serwer administracyjny działa jako punkt dystrybucji.
- Jeden Serwer administracyjny z punktami dystrybucji. Wszystkie urządzenia klienckie są połączone z jednym Serwerem administracyjnym. Niektóre urządzenia klienckie w sieci działają jako punkty dystrybucji.
- Hierarchia Serwerów administracyjnych. Dla każdego segmentu sieci przydzielony jest pojedynczy Serwer administracyjny, który staje się częścią ogólnej hierarchii Serwerów administracyjnych. Główny Serwer administracyjny działa jako punkt dystrybucji.
- Hierarchia Serwerów administracyjnych z punktami dystrybucji. Dla każdego segmentu sieci przydzielony jest pojedynczy Serwer administracyjny, który staje się częścią ogólnej hierarchii Serwerów administracyjnych. Niektóre urządzenia klienckie w sieci działają jako punkty dystrybucji.

Standardowa konfiguracja Kaspersky Security Center

Ta sekcja opisuje standardowe konfiguracje używane podczas wdrażania komponentów Kaspersky Security Center w sieci organizacji:

- Jedno biuro

- Kilka dużych oddziałów, które są oddalone geograficznie od siebie i posiadają swoich własnych administratorów
- Wiele małych biur, które są oddalone geograficznie od siebie

Standardowa konfiguracja: Jedno biuro

W sieci organizacji można zainstalować jeden lub kilka Serwerów administracyjnych. Liczba Serwerów administracyjnych może zostać wybrana w oparciu o dostępny sprzęt lub całkowitą liczbę zarządzanych urządzeń.

Jeden Serwer administracyjny może obsługiwać maksymalnie 100 000 urządzeń. Należy rozważyć możliwość zwiększenia liczby zarządzanych urządzeń w najbliższej przyszłości: wygodniejsze może być podłączenie do jednego Serwera administracyjnego mniejszej liczby urządzeń.

Serwery administracyjne mogą być instalowane w sieci wewnętrznej lub w strefie DMZ, w zależności od tego, czy wymagany jest dostęp do Serwera administracyjnego przez Internet.

Jeśli jest używanych kilka Serwerów, zalecane jest połączenie ich w hierarchię. Korzystanie z hierarchii Serwerów administracyjnych pozwala uniknąć mieszania profili i zadań oraz zarządzać całym zbiorem zarządzanych urządzeń tak, jakby były zarządzane przez jeden Serwer administracyjny (czyli wyszukiwać urządzenia, tworzyć wybory urządzeń oraz generować raporty).

Standardowa konfiguracja: Duże oddziały posiadające swoich administratorów

Jeśli organizacja posiada kilka dużych oddziałów, które są oddalone geograficznie od siebie, należy uwzględnić opcję wdrożenia Serwerów administracyjnych w każdym z biur. W jednym biurze można wdrożyć jeden lub kilka Serwerów administracyjnych, w zależności od liczby urządzeń klienckich i dostępnego sprzętu. W tym przypadku, dla każdego z biur można przeprowadzić „Standardową konfigurację:Jedno biuro". Aby ułatwić zarządzanie, zalecane jest połączenie wszystkich Serwerów administracyjnych w hierarchię (najlepiej wielopoziomową).

Jeśli niektórzy pracownicy poruszają się między biurami ze swoimi urządzeniami (laptopami), w zasadzie Agenta sieciowego należy utworzyć regułę przełączania Agenta sieciowego między Serwerami administracyjnymi.

Standardowa konfiguracja: Małe zdalne biura

Ta standardowa konfiguracja została utworzona z myślą o głównej siedzibie i wielu małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem Internetu. Każde z tych zdalnych biur może znajdować się poza NAT (Network Address Translation - translacja adresów sieciowych), czyli nie można nawiązać połączenia między dwoma zdalnymi biurami, gdyż są odizolowane.

W głównej siedzibie należy zainstalować Serwer administracyjny, natomiast we wszystkich pozostałych biurach należy przydzielić jeden lub kilka punktów dystrybucji. Jeśli biura są połączone przez Internet, przydatne może być utworzenie zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* do punktów dystrybucji, aby mogły one pobierać uaktualnienia bezpośrednio z serwerów Kaspersky, folderu lokalnego lub sieciowego, a nie z Serwera administracyjnego.

Jeśli niektóre urządzenia w zdalnym biurze nie mają bezpośredniego dostępu do Serwera administracyjnego (na przykład, dostęp do Serwera administracyjnego jest możliwy przez Internet, ale niektóre urządzenia nie mają dostępu do Internetu), punkty dystrybucji muszą zostać przełączone do trybu bramy połączenia. W tym przypadku Agenty sieciowe na urządzeniach w zdalnym biurze zostaną połączone, w celu dalszej synchronizacji, z Serwerem administracyjnym, ale poprzez bramę, a nie bezpośrednio.

Ponieważ Serwer administracyjny najprawdopodobniej nie będzie mógł przeszukać sieci zdalnego biura, zalecane jest przekazanie tej funkcji punktowi dystrybucji.

Serwer administracyjny nie będzie mógł wysyłać powiadomień poprzez port UDP o numerze 15000 na zarządzane urządzenia znajdujące się poza NAT w zdalnym biurze. Aby rozwiązać ten problem, we właściwościach urządzeń pełniących rolę punktów dystrybucji możesz włączyć tryb stałego połączenia z Serwerem administracyjnym (pole **Nie odłączaj od Serwera administracyjnego**). Ten tryb jest dostępny, jeśli całkowita liczba punktów dystrybucji nie przekracza 300.

Instalowanie systemu zarządzania bazą danych

Zainstaluj system zarządzania bazą danych (DBMS), który będzie używany przez Kaspersky Security Center. W tym celu wybierz obsługiwany DBMS. Możesz wybrać na przykład PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL lub MariaDB.

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

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

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

Wybieranie systemu zarządzania bazą danych

Podczas wybierania systemu zarządzania bazą danych (DBMS), który zostanie użyty przez Serwer administracyjny, należy brać pod uwagę liczbę urządzeń podlegających Serwerowi administracyjnemu.

Poniższa tabela zawiera listę prawidłowych opcji DBMS, a także zalecenia i ograniczenia dotyczące ich używania.

Zalecenia i ograniczenia dotyczące DBMS

DBMS	Zalecenia i ograniczenia
SQL Server Express Edition 2012 lub nowszy	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 10 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń. Jednoczesne korzystanie z systemu DBMS serwera SQL Server Express Edition przez Serwer administracyjny i inną aplikację jest surowo zabronione.
Lokalny serwer SQL Server inny niż Express, 2012 lub nowszy	Brak ograniczeń.
Zdalny serwer SQL Server inny niż Express, 2012 lub nowszy	Ważne tylko wtedy, gdy oba urządzenia są w tej samej domenie Windows®; jeśli domeny są inne, należy nawiązać między nimi obustronną relację zaufania.
Lokalny lub zdalny MySQL 5.5, 5.6 lub 5.7 (MySQL w wersjach 5.5.1, 5.5.2, 5.5.3, 5.5.4 i 5.5.5 nie jest już obsługiwany)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 10 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń.
Lokalny lub zdalny MySQL 8.0.20 lub nowszy	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 50 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń.

Lokalny lub zdalny MariaDB (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 20 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń.
PostgreSQL, Postgres Pro (zobacz obsługiwane wersje)	Użyj jednego z tych DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 50 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń.

Jeśli używasz SQL Server 2019 jako DBMS, a nie masz łaty zbiorczej CU12 lub nowszej, po zainstalowaniem Kaspersky Security Center powinieneś wykonać następujące czynności:

1. Nawiąż połączenie z SQL Server przy użyciu SQL Management Studio.
2. Uruchom następujące polecenia (jeśli wybrałeś inną nazwę dla bazy danych, użyj nazwy zamiast KAV):

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. Uruchom ponownie usługę SQL Server 2019.

W przeciwnym razie, korzystanie z SQL Server 2019 może zakończyć się błędem, takim jak „There is insufficient system memory in resource pool 'internal' to run this query".

Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 obsługuje MariaDB DBMS. Aby uzyskać więcej informacji na temat obsługiwanych wersji MariaDB, zobacz sekcję Wymagania sprzętowe i programowe.

Jeśli używasz serwera MariaDB dla Kaspersky Security Center, włącz obsługę InnoDB i pamięci MEMORY oraz kodowania UTF-8 i UCS-2.

Zalecane ustawienia dla pliku my.ini

W celu skonfigurowania pliku my.ini:

1. Otwórz plik my.ini w dowolnym edytorze tekstu.
2. Dodaj następujące wiersze do sekcji `[mysqld]` pliku my.ini:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<wartość>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
```

```
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Wartość `innodb_buffer_pool_size` nie może być mniejsza niż 80 procent oczekiwanego rozmiaru bazy danych KAV. Należy pamiętać, że określona pamięć jest przydzielana podczas uruchamiania serwera. Jeśli rozmiar bazy danych jest mniejszy niż określony rozmiar bufora, przydzielana jest tylko wymagana pamięć. Jeśli używasz MariaDB w wersji 10.4.3 lub starszej, rzeczywisty rozmiar przydzielonej pamięci jest o około 10 procent większy niż określony rozmiar bufora.

Zalecane jest użycie wartości parametru `innodb_flush_log_at_trx_commit=0`, ponieważ wartości „1" lub „2" negatywnie wpływają na prędkość działania MariaDB.

Domyślnie dodatki optymalizujące `join_cache_incremental`, `join_cache_hashed` i `join_cache_bka` są włączone. Jeśli te dodatki nie są włączone, musisz je włączyć.

W celu sprawdzenia, czy dodatki optymalizujące są włączone:

1. W konsoli klienta MariaDB wykonaj polecenie:

   ```
   SELECT @@optimizer_switch;
   ```

2. Sprawdź, czy jego dane wyjściowe zawierają następujące wiersze:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Jeśli te wiersze są obecne i mają wartość `on`, to dodatki optymalizujące są włączone.

   Jeśli tych wierszy brakuje lub mają one wartość `off`, wykonaj następujące czynności:

   1. Otwórz plik my.ini w dowolnym edytorze tekstu.

   2. Dodaj następujące wiersze do sekcji `[mysqld]` pliku my.ini:

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

Dodatki `join_cache_incremental`, `join_cache_hash` i `join_cache_bka` są włączone.

Konfigurowanie serwera MySQL x64 do pracy z Kaspersky Security Center 14.2

Jeśli używasz serwera MySQL dla Kaspersky Security Center, włącz obsługę InnoDB i pamięci MEMORY oraz kodowania UTF-8 i UCS-2.

Zalecane ustawienia dla pliku my.ini

W celu skonfigurowania pliku my.ini:

1. Otwórz plik my.ini w dowolnym edytorze tekstu.

2. Dodaj następujące wiersze do sekcji `[mysqld]` pliku my.ini:

   ```
   sort_buffer_size = 10M
   join_buffer_size = 20M
   tmp_table_size = 600M
   max_heap_table_size = 600M
   ```

```
key_buffer_size = 200M
innodb_buffer_pool_size = the real value must be no less than 80% of the expected KAV
database size
innodb_thread_concurrency = 20
innodb_flush_log_at_trx_commit = 0 (in most cases, the server uses small
transactions)
innodb_lock_wait_timeout = 300
max_allowed_packet = 32M
max_connections = 151
max_prepared_stmt_count = 12800
table_open_cache = 60000
table_open_cache_instances = 4
table_definition_cache = 60000
```

Należy pamiętać, że określona w wartości `innodb_buffer_pool_size` pamięć jest przydzielana podczas uruchamiania serwera. Jeśli rozmiar bazy danych jest mniejszy niż określony rozmiar bufora, przydzielana jest tylko wymagana pamięć. Rzeczywisty rozmiar przydzielonej pamięci jest o około 10 procent większy niż określony rozmiar bufora. Więcej informacji można znaleźć w dokumentacji MySQL.

Zalecane jest użycie wartości parametru `innodb_flush_log_at_trx_commit = 0`, ponieważ wartości „1” lub „2” negatywnie wpływają na prędkość działania MySQL.

Konfigurowanie serwera PostgreSQL lub Postgres Pro do pracy z Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 obsługuje DBMS PostgreSQL i Postgres Pro. Jeśli używasz jednego z tych systemów DBMS, rozważ skonfigurowanie parametrów serwera DBMS w celu optymalizacji pracy DBMS z Kaspersky Security Center.

Domyślna ścieżka do pliku konfiguracyjnego to: /etc/postgresql/<WERSJA>/main/postgresql.conf

Zalecane parametry w przypadku PostgreSQL i Postgres Pro:

- `shared_buffers` = 25% wielkości pamięci RAM urządzenia, na którym jest zainstalowany DBMS

  Jeśli pamięć RAM to mniej niż 1 GB, pozostaw wartość domyślną.
- `huge_pages = try`
- `max_stack_depth = 2MB`
- `temp_buffers = 24MB`
- `max_prepared_transactions = 0`
- `work_mem = 16MB`
- `temp_file_limit = -1`
- `max_connections = 151`
- `fsync = on`

Zrestartuj lub przeładuj serwer po zaktualizowaniu pliku postgresql.conf, aby zastosować zmiany. Więcej informacji można znaleźć w dokumentacji PostgreSQL .

Zapoznaj się z następującym tematem, aby uzyskać szczegółowe informacje na temat tworzenia i konfigurowania kont dla PostgreSQL i Postgres Pro: Konfigurowanie kont do pracy z PostgreSQL i Postgres Pro.

Aby uzyskać szczegółowe informacje na temat parametrów serwerów PostgreSQL i Postgres Pro oraz sposobu określania ich, zapoznaj się z odpowiednią dokumentacją DBMS.

Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android

Urządzenia mobilne z zainstalowanym programem Kaspersky Endpoint Security for Android™ (zwane dalej "urządzenia KES") są zarządzane przy użyciu Serwera administracyjnego. Kaspersky Security Center obsługuje następujące funkcje zarządzania urządzeniami KES:

- Zarządzanie urządzeniami mobilnymi jak urządzeniami klienckimi:
  - Członkostwo w grupach administracyjnych
  - Monitorowanie, takie jak przeglądanie stanów, zdarzeń i raportów
  - Modyfikowanie ustawień lokalnych i przydzielanie zasad dla Kaspersky Endpoint Security for Android
- Wysyłanie poleceń w sposób scentralizowany
- Zdalne instalowanie pakietów aplikacji mobilnych

Serwer administracyjny zarządza urządzeniami KES przez TLS, port TCP 13292.

Umożliwianie uzyskania dostępu do Serwera administracyjnego przez internet

Wykonanie następujących czynności wymaga dostępu do Serwera administracyjnego przez Internet:

- Regularne aktualizowanie baz danych, modułów oprogramowania i aplikacji Kaspersky
- Aktualizowanie oprogramowania firm trzecich

  Domyślnie połączenie internetowe w przypadku Serwera administracyjnego nie jest wymagane w celu instalowania aktualizacji oprogramowania firmy Microsoft na zarządzanych urządzeniach. Na przykład zarządzane urządzenia mogą pobierać aktualizacje oprogramowania firmy Microsoft bezpośrednio z serwerów Microsoft Update lub z systemu Windows Server z programem Microsoft Windows Server Update Services (WSUS) wdrożonymi w sieci organizacji. Serwer administracyjny musi być połączony z Internetem w następujących przypadkach:
  - Używanie Serwera administracyjnego jako serwera WSUS
  - Instalowanie aktualizacji oprogramowania firm trzecich innego niż oprogramowanie firmy Microsoft
- Eliminowanie luk w oprogramowaniu innych firm

  Połączenie internetowe w przypadku Serwera administracyjnego jest wymagane, aby można było wykonywać następujące zadania:
  - Sporządzanie listy zalecanych poprawek dla luk w oprogramowaniu firmy Microsoft. Lista jest tworzona i regularnie aktualizowana przez specjalistów z Kaspersky.

    - Naprawianie luk w oprogramowaniu firm trzecich innym niż oprogramowanie firmy Microsoft.
- Zarządzanie urządzeniami (laptopami) użytkowników mobilnych
- Zarządzanie urządzeniami w zdalnych biurach
- Komunikowanie się z głównym lub podrzędnym Serwerem administracyjnym w zdalnych biurach
- Zarządzanie urządzeniami mobilnymi

Ta sekcja opisuje podstawowe sposoby zapewnienia dostępu do Serwera administracyjnego poprzez Internet. W każdym przypadku skupiającym się na zapewnieniu Serwerowi administracyjnemu dostępu do Internetu może być wymagany dedykowany certyfikat dla Serwera administracyjnego.

Dostęp do internetu: Serwer administracyjny w sieci lokalnej

Jeśli Serwer administracyjny znajduje się w wewnętrznej sieci organizacji, możesz udostępnić port TCP o numerze 13000 Serwera administracyjnego z zewnątrz za pomocą przekierowania portów. Jeśli wymagane jest zarządzanie urządzeniami mobilnymi, możesz udostępnić port 13292 TCP.

Dostęp do internetu: Serwer administracyjny w strefie DMZ

Jeśli Serwer administracyjny znajduje się w DMZ sieci organizacji, nie ma on dostępu do wewnętrznej sieci organizacji. Dlatego też występują następujące ograniczenia:

- Serwer administracyjny nie może wykryć nowych urządzeń.
- Serwer administracyjny nie może wykonać wstępnej instalacji Agenta sieciowego przy użyciu wymuszonej instalacji na urządzeniach w wewnętrznej sieci organizacji.

Dotyczy to tylko wstępnej instalacji Agenta sieciowego. Jednakże jakiekolwiek późniejsze uaktualnienia Agenta sieciowego lub instalacja aplikacji zabezpieczającej mogą zostać wykonane przez Serwer administracyjny. Jednocześnie, wstępna instalacja Agentów sieciowych może odbyć się, na przykład, poprzez zasady grupy Microsoft® Active Directory®.

- Serwer administracyjny nie może wysyłać powiadomień na zarządzane urządzenia poprzez port UDP o numerze 15000, co nie jest krytyczne dla działania Kaspersky Security Center.
- Serwer administracyjny nie może przeszukiwać Active Directory. Jednakże w większości scenariuszy wyniki przeszukiwania Active Directory nie są wymagane.

Jeśli powyższe ograniczenia są postrzegane jako krytyczne, można je znieść przy pomocy punktów dystrybucji znajdujących się w sieci organizacji:

- Aby przeprowadzić wstępną instalację na urządzeniach bez Agenta sieciowego, w pierwszej kolejności zainstaluj Agenta sieciowego na jednym z urządzeń, a następnie przypisz mu stan punktu dystrybucji. W rezultacie, wstępna instalacja Agenta sieciowego na pozostałych urządzeniach zostanie przeprowadzona przez Serwer administracyjny poprzez ten punkt dystrybucji.
- Aby wykrywać nowe urządzenia w wewnętrznej sieci organizacji i przeszukiwać Active Directory, w jednym z punktów dystrybucji musisz włączyć odpowiednie metody wykrywania urządzeń.

Aby zapewnić pomyślne wysyłanie powiadomień przez port UDP o numerze 15000 na zarządzane urządzenia znajdujące się w wewnętrznej sieci organizacji, musisz wypełnić całą swoją sieć punktami dystrybucji. We właściwościach przypisanych punktów dystrybucji zaznacz pole **Nie odłączaj od Serwera administracyjnego**. Serwer administracyjny nawiąże stale połączenie z punktami dystrybucji, które będą mogły wysyłać powiadomienia poprzez port UDP o numerze 15000 na urządzenia, które znajdują się w wewnętrznej sieci organizacji (to może być.sieć IPv4 lub IPv6).

Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej

Serwer administracyjny może znajdować się w wewnętrznej sieci organizacji, w strefie zdemilitaryzowanej (DMZ), gdzie może być urządzenie z Agentem sieciowym działającym jako brama połączenia z odwróconym połączeniem (Serwer administracyjny nawiązuje połączenie z Agentem sieciowym). W tym przypadku, w celu zapewnienia dostępu do Internetu muszą zostać spełnione następujące warunki:

- Agent sieciowy musi być zainstalowany na urządzeniu, które znajduje się w DMZ. Jeśli instalujesz Agenta sieciowego, w oknie **Brama połączenia** kreatora instalacji wybierz **Użyj Agenta sieciowego jako bramy połączenia w DMZ**.
- Urządzenie z zainstalowaną bramą połączenia musi zostać dodane do punktu dystrybucji. Po dodaniu bramy połączeniu, w oknie **Dodaj punkt dystrybucji** wybierz opcję **Wybierz → Dodaj bramę połączenia w DMZ na podstawie adresu**.
- Aby używać połączenia internetowego do podłączania zewnętrznych komputerów stacjonarnych z Serwerem administracyjnym, należy poprawić pakiet instalacyjny Agenta sieciowego. We właściwościach utworzonego pakietu instalacyjnego wybierz opcję **Zaawansowane → Połącz z Serwerem administracyjnym korzystając z bramy połączenia**, a następnie określ nowo utworzoną bramę połączenia.

Dla bramy połączenia w strefie DMZ Serwer administracyjny tworzy certyfikat podpisany przez certyfikat Serwera administracyjnego. Jeśli administrator zdecyduje przydzielić Serwerowi administracyjnemu certyfikat niestandardowy, musi to zrobić przed utworzeniem bramy połączenia w strefie DMZ.

Jeśli niektórzy pracownicy korzystają z laptopów, które mogą łączyć się z Serwerem administracyjnym z sieci lokalnej lub poprzez Internet, przydatne będzie utworzenie w zasadzie Agenta sieciowego reguły przełączania dla Agenta sieciowego.

Informacje o punktach dystrybucji

Urządzenie z zainstalowanym Agentem sieciowym może być używane jako punkt dystrybucji. W tym trybie Agent sieciowy może wykonywać następujące funkcje:

- Rozsyłać uaktualnienia (mogą być one pobierane z Serwera administracyjnego lub z serwerów Kaspersky). W drugim przypadku należy utworzyć zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* dla urządzenia pełniącego rolę punktu dystrybucji:
  - Instalować oprogramowanie (włączając w to wstępną instalację Agentów sieciowych) na pozostałych urządzeniach.
  - Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może stosować te same metody wykrywania urządzeń co Serwer administracyjny.

Instalacja punktów dystrybucji w sieci organizacji realizuje następujące cele:

- Zmniejszanie obciążenia na Serwerze administracyjnym.
- Optymalizowanie ruchu sieciowego.

- Zapewnienie Serwerowi administracyjnemu dostępu do urządzeń w ciężko dostępnych miejscach sieci organizacji. Dostępność punktu dystrybucji w sieci poza NAT (w powiązaniu z Serwerem administracyjnym) umożliwia Serwerowi administracyjnemu wykonywanie następujących działań:
  - Wysyłanie powiadomień do urządzeń przez UDP w sieci IPv4 lub IPv6
  - Przeszukiwanie sieci IPv4 lub IPv6
  - Przeprowadzanie wstępnej konfiguracji
  - Pełnienie funkcji serwera push

Punkt dystrybucji jest przydzielony do grupy administracyjnej. W tym przypadku zakres działania punktu dystrybucji obejmuje wszystkie urządzenia w grupie administracyjnej i jej podgrupach. Jednakże urządzenie pełniące funkcję punktu dystrybucji może nie znajdować się w grupie administracyjnej, do której zostało przydzielone.

Możesz sprawić, że punkt dystrybucji będzie działał jako brama połączenia. W tym przypadku urządzenia objęte zakresem działania punktu dystrybucji będą łączyły się z Serwerem administracyjnym poprzez bramę, a nie bezpośrednio. Ten tryb może być przydatny w scenariuszach, które nie zezwalają na nawiązywanie bezpośredniego połączenia między Serwerem administracyjnym a zarządzanymi urządzeniami.

Obliczanie liczby i konfigurowanie punktów dystrybucji

Im więcej urządzeń klienckich zawiera sieć, tym więcej punktów dystrybucji wymaga. Nie jest zalecane wyłączanie automatycznego przypisywania punktów dystrybucji. Jeśli automatyczne przypisywanie punktów dystrybucji jest włączone, Serwer administracyjny przypisuje punkty dystrybucji, gdy liczba urządzeń klienckich jest dosyć duża, oraz definiuje ich konfigurację.

Używanie specjalnie przypisanych punktów dystrybucji

Jeśli planujesz używać określonych urządzeń jako punktów dystrybucji (na przykład, specjalnie wybranych serwerów), możesz zrezygnować z automatycznego przypisywania punktów dystrybucji. W tym przypadku upewnij się, że na urządzeniach, które mają pełnić rolę punktów dystrybucji, jest wystarczająca ilość wolnego miejsca, nie są regularnie wyłączane, a tryb uśpienia jest na nich wyłączony.

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–100	1
Więcej niż 100	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Korzystanie ze standardowych urządzeń klienckich (stacji roboczych) jako punktów dystrybucji

Jeśli planujesz używać standardowych urządzeń klienckich (czyli stacji roboczych) jako punktów dystrybucji, zalecane jest przypisanie punktów dystrybucji w sposób pokazany w tabelach poniżej, aby uniknąć nadmiernego obciążenia kanałów komunikacji i Serwera administracyjnego:

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–30	1
31–300	2
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Jeśli punkt dystrybucji jest wyłączony (lub z jakiegoś powodu niedostępny), zarządzane urządzenia w tym obszarze mogą uzyskać dostęp do Serwera administracyjnego w celu pobrania uaktualnień.

Hierarchia Serwerów administracyjnych

W MSP może działać kilka Serwerów administracyjnych. Niewygodne może być zarządzanie kilkoma oddzielnymi Serwerami administracyjnymi, dlatego dobrym wyjściem jest utworzenie hierarchii. Zastosowanie konfiguracji „główny/podrzędny" dla dwóch Serwerów administracyjnych oferuje następujące możliwości:

- Podrzędny Serwer administracyjny dziedziczy profile i zadania od głównego Serwera administracyjnego, zapobiegając dzięki temu powielaniu ustawień.
- Wybory urządzeń na głównym Serwerze administracyjnym mogą zawierać urządzenia z podrzędnych Serwerów administracyjnych.
- Raporty na głównym Serwerze administracyjnym mogą zawierać dane (w tym szczegółowe informacje) z podrzędnych Serwerów administracyjnych.

Wirtualne Serwery administracyjne

W oparciu o fizyczny Serwer administracyjny można utworzyć kilka wirtualnych Serwerów administracyjnych, które będą podobne do podrzędnych Serwerów administracyjnych. W przeciwieństwie do trybu poufnego dostępu, który jest oparty na listach kontroli dostępu (ACL), tryb wirtualnego Serwera administracyjnego jest bardziej funkcjonalny i zapewnia większy stopień izolacji. Jako dodatek do dedykowanej struktury grup administracyjnych dla przypisanych urządzeń z zasadami i zadaniami, każdy wirtualny Serwer administracyjny zawiera swoją grupę nieprzypisanych urządzeń, własne zestawy raportów, wybranych urządzeń i zdarzeń, pakietów instalacyjnych, reguł przenoszenia itd. Zasięg działania wirtualnego Serwera administracyjnego może być wykorzystany przez dostawców usług (xSP) do zwiększenia izolacji klientów, a także przez organizacje działające na szeroką skalę z zaawansowanym przepływem pracy i dużą liczbą administratorów.

Wirtualne Serwery administracyjne są bardzo podobne do podrzędnych Serwerów administracyjnych, jednakże posiadają pewne różnice:

- Wirtualny Serwer administracyjny nie posiada większości ustawień globalnych i swoich własnych portów TCP.
- Wirtualny Serwer administracyjny nie posiada podrzędnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny nie posiada innych wirtualnych Serwerów administracyjnych.
- Fizyczny Serwer administracyjny wyświetla urządzenia, grupy, zdarzenia i obiekty na zarządzanych urządzeniach (elementy w Kwarantannie, rejestrze aplikacji itd.) ze wszystkich swoich wirtualnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny może skanować sieć wyłącznie przy podłączonych punktach dystrybucji.

Informacje o ograniczeniach Kaspersky Security Center

Poniższa tabela wyświetla ograniczenia bieżącej wersji Kaspersky Security Center.

Ograniczenia Kaspersky Security Center

Rodzaj ograniczenia	Wartość
Maksymalna liczba zarządzanych urządzeń na Serwer administracyjny	100 000
Maksymalna liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego**	300
Maksymalna liczba grup administracyjnych	10 000
Maksymalna liczba przechowywanych zdarzeń	45 000 000
Maksymalna liczba profili	2000
Maksymalna liczba zadań	2000
Maksymalna całkowita liczba obiektów Active Directory (jednostek organizacyjnych i kont użytkowników, urządzeń oraz grup bezpieczeństwa)	1 000 000
Maksymalna liczba profili w zasadzie	100
Maksymalna liczba podrzędnych Serwerów administracyjnych w jednym głównym Serwerze administracyjnym	500
Maksymalna liczba wirtualnych Serwerów administracyjnych	500
Maksymalna liczba urządzeń, jaką obejmuje pojedynczy punkt dystrybucji (punkty dystrybucji mogą obejmować tylko urządzenia niemobilne)	10 000
Maksymalna liczba urządzeń, które mogą używać pojedynczej bramy połączenia	10 000, w tym urządzenia mobilne
Maksymalna liczba urządzeń mobilnych na Serwer administracyjny	100 000 minus liczba

	stacjonarnych zarządzanych urządzeń

Obciążenie sieci

Ta sekcja zawiera informacje o ilości ruchu sieciowego wymienianego między urządzeniami klienckimi a Serwerem administracyjnym podczas wykonywania kluczowych działań administracyjnych.

Największe obciążenie sieci jest wywoływane przez realizację następujących scenariuszy administracyjnych:

- Wstępna zdalna instalacja ochrony antywirusowej
- Wstępna aktualizacja baz danych programu antywirusowego
- Synchronizacja urządzenia klienckiego z Serwerem administracyjnym
- Regularna aktualizacja antywirusowych baz danych
- Przetwarzanie zdarzeń występujących na urządzeniach klienckich przez Serwer administracyjny

Wstępna zdalna instalacja ochrony antywirusowej

Ta sekcja zawiera informacje o rozmiarze ruchu sieciowego po zainstalowaniu na urządzeniu klienckim Agenta sieciowego i programu Kaspersky Endpoint Security for Windows (zobacz poniższą tabelę).

Agent sieciowy jest instalowany przy użyciu instalacji wymuszonej, podczas której pliki potrzebne do przeprowadzenia instalacji są kopiowane z Serwera administracyjnego do folderu współdzielonego na urządzeniu klienckim. Po instalacji, Agent sieciowy pobiera pakiet dystrybucyjny Kaspersky Endpoint Security for Windows, korzystając z połączenia z Serwerem administracyjnym.

Ruch sieciowy

Scenariusz	Instalacja Agenta sieciowego na pojedynczym urządzeniu klienckim	Instalowanie Kaspersky Endpoint Security for Windows na jednym urządzeniu klienckim (z aktualizacją baz danych)	Równoległa instalacja Agenta sieciowego i Kaspersky Endpoint Security for Windows
Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego, KB	1638,4	7843,84	9707,52
Ruch sieciowy z Serwera administracyjnego do urządzenia klienckiego, KB	69 990,4	259 317,76	329 318,4
Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego), KB	71 628,8	267 161,6	339 025,92

Po zainstalowaniu Agentów sieciowych na urządzeniach klienckich, jedno z urządzeń należących do grupy administracyjnej może być wyznaczone do pełnienia roli punktu dystrybucji. Będzie ono używane do rozsyłania pakietów instalacyjnych. W tej sytuacji rozmiar ruchu sieciowego przesyłanego podczas wstępnej zdalnej instalacji ochrony antywirusowej będzie się znacznie różnił w zależności od tego, czy używana jest multiemisja IP.

Jeśli multiemisja IP jest używana, pakiety instalacyjne tylko raz zostają wysłane do wszystkich uruchomionych urządzeń należących do grupy administracyjnej. Z tego powodu całkowity ruch sieciowy będzie N razy mniejszy, gdzie N oznacza całkowitą liczbę uruchomionych urządzeń należących do grupy administracyjnej. W przypadku, gdy funkcja multiemisji IP nie jest używana, całkowity ruch sieciowy jest podobny do ruchu sieciowego podczas pobierania pakietów dystrybucyjnych z Serwera administracyjnego. Jednakże źródłem pakietu będzie punkt dystrybucji, a nie Serwer administracyjny.

Wstępna aktualizacja baz danych programu antywirusowego

Ilość ruchu sieciowego podczas początkowej aktualizacji antywirusowych baz danych (podczas pierwszego uruchomienia zadania aktualizacji baz danych na urządzeniu klienckim) jest następująca:

- Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego: 1,8 MB.
- Ruch sieciowy z Serwera administracyjnego do urządzenia klienckiego: 113 MB.
- Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego): 114 MB.

Dane mogą się nieznacznie różnić w zależności od bieżącej wersji antywirusowych baz danych.

Synchronizowanie klienta z Serwerem administracyjnym

Scenariusz ten opisuje stan systemu administracyjnego w sytuacji, gdy zachodzi intensywna synchronizacja danych pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Urządzenia klienckie nawiązują połączenie z Serwerem administracyjnym w przedziale czasowym określonym przez administratora. Serwer administracyjny porównuje stan danych na urządzeniu klienckim ze stanem danych na Serwerze, zapisuje w bazie danych informacje o ostatnim połączeniu urządzenia klienckiego i przeprowadza synchronizację danych.

Ta sekcja zawiera informacje o rozmiarach ruchu dla podstawowych scenariuszy administracyjnych przy łączeniu klienta z Serwerem administracyjnym (zobacz poniższą tabelę). Dane znajdujące się w tabeli mogą się nieznacznie różnić w zależności od bieżącej wersji antywirusowych baz danych.

Ruch sieciowy

Scenariusz	Ruch sieciowy z urządzeń klienckich do Serwera administracyjnego, KB	Ruch sieciowy z Serwera administracyjnego do urządzeń klienckich, KB	Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego), KB
Wstępna synchronizacja przed aktualizacją baz danych na urządzeniu klienckim	699,44	568,42	1267,86
Wstępna synchronizacja po aktualizacji baz danych na urządzeniu klienckim	735,8	4474,88	5210,68
Synchronizacja bez zmian na urządzeniu klienckim i Serwerze administracyjnym	11,99	6,73	18,72
Synchronizacja po zmianie wartości ustawień w profilu grupy	9,79	11,39	21,18

Synchronizacja po zmianie wartości ustawień w zadaniu grupowym	11,27	11,72	22,99
Wymuszona synchronizacja bez zmian na urządzeniu klienckim	77,59	99,45	177,04

Całkowita ilość ruchu sieciowego może znacznie się wahać, w zależności od tego, czy w grupach administracyjnych wykorzystywana jest opcja multiemisji IP. Jeśli opcja ta jest używana, całkowity rozmiar ruchu sieciowego będzie o około N razy mniejszy dla grupy, gdzie N oznacza całkowitą liczbę urządzeń należących do grupy administracyjnej.

Ilość ruchu sieciowego przy wstępnej synchronizacji przed i po aktualizacji baz danych jest określona dla następujących przypadków:

- Instalowanie Agenta sieciowego i aplikacji zabezpieczającej na urządzeniu klienckim
- Przenoszenie urządzenia klienckiego do grupy administracyjnej
- Stosowanie do urządzenia klienckiego profilu i zadań domyślnie utworzonych dla grupy

Tabela określa szybkość ruchu sieciowego w przypadku zmian wprowadzonych w jednym z ustawień ochrony, które znajdują się w ustawieniach profilu Kaspersky Endpoint Security. Dane dla innych ustawień profilu mogą się różnić od danych wyświetlonych w tabeli.

Dodatkowa aktualizacja baz danych programu antywirusowego

Rozmiar ruchu sieciowego w przypadku inkrementacyjnych aktualizacji antywirusowych baz danych po 20 godzinach od poprzedniej aktualizacji wygląda następująco:

- Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego: 169 KB.
- Ruch sieciowy z Serwera administracyjnego do urządzenia klienckiego: 16 MB.
- Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego): 16.3 MB.

Dane znajdujące się w tabeli mogą się nieznacznie różnić w zależności od bieżącej wersji antywirusowych baz danych.

Ilość ruchu sieciowego może znacznie się wahać, w zależności od tego, czy w grupach administracyjnych wykorzystywana jest opcja multiemisji IP. Jeśli opcja ta jest używana, całkowity rozmiar ruchu sieciowego będzie o około N razy mniejszy dla grupy, gdzie N oznacza całkowitą liczbę urządzeń należących do grupy administracyjnej.

Przetwarzanie zdarzeń występujących na klientach przez Serwer administracyjny

Ta sekcja zawiera informacje o ilości ruchu sieciowego, gdy na urządzeniu klienckim wystąpi zdarzenie „Wykryto wirusa", które jest wysyłane do Serwera administracyjnego i jest rejestrowane w jego bazie danych (patrz tabela poniżej).

Ruch sieciowy

Scenariusz	Przesyłanie danych do Serwera administracyjnego po wystąpieniu zdarzenia „Wykryto wirusa"	Przesyłanie danych do Serwera administracyjnego po wystąpieniu dziewięciu zdarzeń „Wykryto wirusa"
Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego, KB	49,66	64,05
Ruch sieciowy z Serwera administracyjnego do	28,64	31,97

urządzenia klienckiego, KB		
Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego), KB	78,3	96,02

Dane znajdujące się w tabeli mogą się nieznacznie różnić w zależności od aktualnej wersji aplikacji antywirusowej oraz zdarzeń, które są zdefiniowane w jej profilu do rejestracji w bazie danych Serwera administracyjnego.

Ruch na 24 godziny

Ta sekcja zawiera informacje o rozmiarach ruchu dla 24 godzin aktywności systemu administracyjnego w warunkach „spokoju", kiedy nie występuje modyfikacja danych na urządzeniach klienckich i na Serwerze administracyjnym (patrz tabela poniżej).

Dane wymienione w tabeli opisują stan sieci po standardowej instalacji Kaspersky Security Center i po zamknięciu kreatora wstępnej konfiguracji. Częstotliwość synchronizacji urządzenia klienckiego z Serwerem administracyjnym wynosiła 20 minut; uaktualnienia były pobierane do repozytorium Serwera administracyjnego co godzinę.

Ilość ruchu sieciowego na 24 godziny w stanie bezczynności

Przepływ ruchu	Wartość
Ruch sieciowy z urządzenia klienckiego do Serwera administracyjnego, KB	3235,84
Ruch sieciowy z Serwera administracyjnego do urządzenia klienckiego, KB	64 378,88
Całkowity ruch sieciowy (dla pojedynczego urządzenia klienckiego), KB	67 614,72

Przygotowywanie do zarządzania urządzeniami mobilnymi

Ta sekcja zawiera następujące informacje:

- Informacje o serwerze urządzeń mobilnych Exchange, przeznaczonym do zarządzania urządzeniami mobilnymi poprzez protokół Exchange ActiveSync
- Informacje o serwerze iOS MDM, przeznaczonym do zarządzania urządzeniami iOS poprzez zainstalowanie na nich dedykowanych profili iOS MDM
- Informacje o zarządzaniu urządzeniami mobilnymi, na których jest zainstalowany Kaspersky Endpoint Security for Android

Serwer urządzeń mobilnych Exchange

Serwer urządzeń mobilnych Exchange umożliwia zarządzanie urządzeniami mobilnymi, które są połączone z Serwerem administracyjnym za pomocą protokołu Exchange ActiveSync (urządzenia EAS).

Instalowanie serwera urządzeń mobilnych Exchange

Jeśli w organizacji zainstalowano kilka serwerów Exchange z obrębu macierzy serwera dostępu klienta, na każdym serwerze w tej macierzy należy zainstalować serwer urządzeń mobilnych Exchange. Opcja **Tryb klastra** musi być włączona w kreatorze wdrażania serwera urządzeń mobilnych Exchange. W tym przypadku zestaw serwerów urządzeń mobilnych Exchange zainstalowanych na serwerach w macierzy będzie określany jako klaster serwerów urządzeń mobilnych Exchange.

Jeśli w organizacji nie zainstalowano żadnej macierzy serwera dostępu klienta Microsoft Exchange Servers, serwer urządzeń mobilnych Exchange musi zostać zainstalowany na serwerze Microsoft Exchange Server, na którym jest dostęp klienta. W tym przypadku w kreatorze instalacji serwera urządzeń mobilnych Exchange włącz opcję **Tryb standardowy**.

Wraz z serwerem urządzeń mobilnych Exchange należy zainstalować Agenta sieciowego, gdyż pomoże to zintegrować serwer urządzeń mobilnych Exchange z Kaspersky Security Center.

Domyślnym obszarem skanowania serwera urządzeń mobilnych Exchange jest bieżąca domena Active Directory, w której został zainstalowany. Instalowanie serwera urządzeń mobilnych Exchange na serwerze z zainstalowanym serwerem Microsoft Exchange Server (wersje 2010, 2013) umożliwia rozszerzenie obszaru skanowania w celu uwzględnienia całego lasu domen na serwerze urządzeń mobilnych Exchange (sekcja „Konfigurowanie obszaru skanowania"). Podczas skanowania wymagane są informacje o kontach użytkowników serwera Microsoft Exchange, profilach Exchange ActiveSync oraz urządzeniach mobilnych użytkowników podłączonych do serwera Microsoft Exchange Server poprzez protokół Exchange ActiveSync.

W jednej domenie nie można zainstalować kilku serwerów urządzeń mobilnych Exchange, jeśli działają w **Tryb standardowy** i są zarządzane przez jeden Serwer administracyjny. W obrębie jednego lasu domeny Active Directory nie można zainstalować kilku serwerów urządzeń mobilnych Exchange (lub kilku klastrów serwerów urządzeń mobilnych Exchange), jeśli działają w **Tryb standardowy** z rozszerzonym obszarem skanowania, który zawiera cały las domen, i jeśli są połączone z jednym Serwerem administracyjnym.

Uprawnienia wymagane do zainstalowania serwera urządzeń mobilnych Exchange

Instalacja serwera urządzeń mobilnych Exchange na serwerze Microsoft Exchange Server (2010, 2013) wymaga uprawnień administratora domeny i roli Zarządzanie organizacją. Instalacja serwera urządzeń mobilnych Exchange na serwerze Microsoft Exchange Server (2007) wymaga uprawnień administratora domeny i członkostwa w grupie zabezpieczeń Administratorzy organizacji programu Exchange.

Konto dla usługi Exchange ActiveSync

Po zainstalowaniu serwera urządzeń mobilnych Exchange, w Active Directory automatycznie tworzone jest konto:

- Na serwerze Microsoft Exchange Server (2010, 2013): konto KLMDM4ExchAdmin***** z rolą KLMDM Role Group.
- Na serwerze Microsoft Exchange Server (2007): konto KLMDM4ExchAdmin***** należące do grupy zabezpieczeń KLMDM Secure Group.

Usługa serwera urządzeń mobilnych Exchange jest uruchamiana z poziomu tego konta.

Jeśli chcesz anulować automatyczne tworzenie konta, musisz utworzyć niestandardowe konto z następującymi uprawnieniami:

- Podczas korzystania z serwera Microsoft Exchange Server (2010, 2013) do konta musi zostać przypisana rola, która może wykonywać następujące polecenia cmdlet:
  - Get-CASMailbox
  - Set-CASMailbox
  - Remove-ActiveSyncDevice
  - Clear-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics

- Get-AcceptedDomain
- Set-AdServerSettings
- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy
- Remove-ActiveSyncMailboxPolicy

- Podczas korzystania z serwera Microsoft Exchange Server (2007) konto musi posiadać uprawnienia dostępu do obiektów Active Directory (patrz poniższa tabela).

Uprawnienia dostępu do obiektów Active Directory

Dostęp	Obiekt	Cmdlet
Pełna	Thread "CN=Mobile Mailbox Policies,CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nazwa domeny>"	`Add-ADPermission -User <Nazwa gru użytkownika> -Identity "CN=Mobile Policies,CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configura <Nazwa domeny>" -InheritanceType AccessRight GenericAll`
Odczyt	Thread "CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nazwa domeny>"	`Add-ADPermission -User <Nazwa gru użytkownika> -Identity "CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configura <Nazwa domeny>" -InheritanceType AccessRight GenericRead`
Odczyt/zapis	Właściwości msExchMobileMailboxPolicyLink i msExchOmaAdminWirelessEnable dla obiektów w Active Directory	`Add-ADPermission -User <Nazwa gru użytkownika> -Identity "DC=<Nazwa domeny>" -InheritanceType All - AccessRight ReadProperty,WritePro Properties msExchMobileMailboxPol msExchOmaAdminWirelessEnable`
Rozszerzone uprawnienia ms-Exch-Store-Active	Mailbox repositories of Exchange server, thread "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nazwa domeny>"	`Get-MailboxDatabase | Add-ADPermi User <Nazwa użytkownika lub grupy ExtendedRights ms-Exch-Store-Admi`

Serwer iOS MDM

Serwer iOS MDM umożliwia zarządzanie urządzeniami iOS poprzez zainstalowane na nich profile iOS MDM. Obsługiwane są następujące funkcje:

- Blokowanie urządzenia
- Resetowanie hasła

- Usuwanie danych
- Instalowanie i dezinstalowanie aplikacji
- Użycie profilu iOS MDM z ustawieniami zaawansowanymi (np. ustawienia VPN, ustawienia e-mail, ustawienia Wi-Fi, ustawienia aparatu, certyfikaty itd.)

Serwer iOS MDM jest usługą sieciową odbierającą połączenia przychodzące z urządzeń mobilnych poprzez swój protokół TLS (domyślne jest to port 443), która jest zarządzana poprzez Kaspersky Security Center przy użyciu Agenta sieciowego. Agent sieciowy jest instalowany lokalnie, na urządzeniu z zainstalowanym serwerem iOS MDM.

Podczas instalacji serwera iOS MDM administrator musi wykonać następujące czynności:

- Zapewnić Agentowi sieciowemu dostęp do Serwera administracyjnego
- Zapewnić urządzeniom mobilnym dostęp do portu TCP serwera iOS MDM

Ta sekcja przedstawia dwie standardowe konfiguracje serwera iOS MDM.

Standardowa konfiguracja: Kaspersky Device Management for iOS w strefie DMZ

Serwer iOS MDM znajduje się w strefie zdemilitaryzowanej (DMZ) sieci lokalnej organizacji z dostępem do Internetu. Specjalną funkcją tej konfiguracji jest brak jakichkolwiek problemów podczas uzyskiwania dostępu do usługi sieciowej iOS MDM z poziomu urządzeń przez Internet.

Ponieważ zarządzanie serwerem iOS MDM wymaga zainstalowania Agenta sieciowego lokalnie, należy zapewnić interakcję Agenta sieciowego z Serwerem administracyjnym. Można to zrobić przy użyciu jednej z następujących metod:

- Przenosząc Serwer administracyjny do strefy DMZ.
- Korzystając z bramy połączenia:

  a. Na urządzeniu z zainstalowanym serwerem iOS MDM połącz Agenta sieciowego z Serwerem administracyjnym poprzez bramę połączenia.

  b. Na urządzeniu z zainstalowanym serwerem iOS MDM wskaż Agenta sieciowego jako bramę połączenia.

Standardowa konfiguracja: Serwer iOS MDM w sieci lokalnej organizacji

Serwer iOS MDM znajduje się w wewnętrznej sieci organizacji. Aby umożliwić dostęp z zewnątrz, należy włączyć port 443 (domyślny port). Można to zrobić, na przykład, publikując usługę sieciową iOS MDM na Microsoft Forefront® Threat Management Gateway (zwany dalej TMG).

Każda standardowa konfiguracja wymaga dla serwera iOS MDM dostępu do usług sieciowych Apple (zakres 17.0.0.0/8) poprzez port TCP 2197. Ten port jest używany do informowania urządzeń o nowych poleceniach przy użyciu dedykowanej usługi o nazwie APNs.

Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android

Urządzenia mobilne z zainstalowanym programem Kaspersky Endpoint Security for Android™ (zwane dalej "urządzenia KES") są zarządzane przy użyciu Serwera administracyjnego. Kaspersky Security Center obsługuje następujące funkcje zarządzania urządzeniami KES:

- Zarządzanie urządzeniami mobilnymi jak urządzeniami klienckimi:

- Członkostwo w grupach administracyjnych
- Monitorowanie, takie jak przeglądanie stanów, zdarzeń i raportów
- Modyfikowanie ustawień lokalnych i przydzielanie zasad dla Kaspersky Endpoint Security for Android

- Wysyłanie poleceń w sposób scentralizowany
- Zdalne instalowanie pakietów aplikacji mobilnych

Serwer administracyjny zarządza urządzeniami KES przez TLS, port TCP 13292.

Informacje o wydajności Serwera administracyjnego

Ta sekcja wyświetla wyniki testów wydajnościowych Serwera administracyjnego dla różnych konfiguracji sprzętowych, a także ograniczenia dotyczące połączenia zarządzanych urządzeń z Serwerem administracyjnym.

Ograniczenia połączenia z Serwerem administracyjnym

Serwer administracyjny obsługuje zarządzanie do 100 000 urządzeń bez straty na wydajności.

Ograniczenia połączeń z Serwerem administracyjnym bez straty na wydajności:

- Jeden Serwer administracyjny może obsługiwać maksymalnie 500 wirtualnych Serwerów administracyjnych.
- Główny Serwer administracyjny obsługuje nie więcej niż 1000 sesji jednocześnie.
- Wirtualne Serwery administracyjne obsługują nie więcej niż 1000 sesji jednocześnie.

Rezultaty testów wydajnościowych Serwera administracyjnego

Rezultaty testów wydajnościowych Serwera administracyjnego pozwoliły określić maksymalną liczbę urządzeń klienckich, z którymi Serwer administracyjny może się zsynchronizować w określonych przedziałach czasu. Informacje te mogą być wykorzystane do stworzenia optymalnego schematu wdrożenia ochrony antywirusowej w sieciach komputerowych.

Podczas testów użyte zostały następujące konfiguracje sprzętowe Serwera administracyjnego (patrz tabele poniżej):

Konfiguracja sprzętowa Serwera administracyjnego

Parametr	Wartość
Procesor	Intel Xeon CPU E5630, częstotliwość taktowania 2.53 GHz, 2 gniazda, 8 rdzeni, 16 procesorów logicznych
Pamięć RAM	26 GB
Dysk twardy	IBM ServeRAID M5014 SCSI Disk Device, 487 GB
System	Microsoft Windows Server 2019 Standard, wersja 10.0.17763, kompilacja 17763

operacyjny	
Sieć	QLogic BCM5709C Gigabit Ethernet (klient NDIS VBD)

Konfiguracja sprzętowa urządzenia z serwerem SQL

Parametr	Wartość
Procesor	Intel Xeon CPU X5570, częstotliwość taktowania 2.93 GHz, 2 gniazda, 8 rdzeni, 16 procesorów logicznych
Pamięć RAM	32 GB
Dysk twardy	Urządzenie dyskowe Adaptec Array SCSI, 2047 GB
System operacyjny	Microsoft Windows Server 2019 Standard, wersja 10.0.17763, kompilacja 17763
Sieć	Intel 82576 Gigabit

Serwer administracyjny obsługiwał tworzenie 500 wirtualnych Serwerów administracyjnych.

Okres synchronizacji wynosił 15 minut dla każdych 10 000 zarządzanych urządzeń (patrz tabela poniżej).

Ogólne rezultaty testów obciążeniowych Serwera administracyjnego

Okres synchronizacji (min)	Liczba zarządzanych urządzeń
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
90	60 000
105	70 000
120	80 000
135	90 000
150	100 000

Jeśli łączysz Serwer administracyjny z serwerem bazodanowym MySQL lub SQL Express, nie zaleca się zarządzać przy pomocy aplikacji liczbą urządzeń większą niż 10 000. W przypadku systemu zarządzania bazą danych MariaDB maksymalna zalecana liczba zarządzanych urządzeń to 20 000.

Wyniki sprawdzania działania serwera KSN proxy

Jeśli Twoja sieć firmowa zawiera dużą liczbę urządzeń klienckich i używają one Serwera administracyjnego jako serwera proxy KSN, sprzęt Serwera administracyjnego musi spełniać określone wymagania, aby możliwe było przetwarzanie żądań z urządzeń klienckich. Możesz wykorzystać wyniki testowania do oceny obciążenia Serwera administracyjnego w swojej sieci i rozplanować zasoby sprzętowe, aby zapewnić normalne funkcjonowanie usługi KSN proxy.

Tabele poniżej pokazują konfigurację sprzętową Serwera administracyjnego i serwera SQL. Ta konfiguracja została użyta do testowania.

Konfiguracja sprzętowa Serwera administracyjnego

Parametr	Wartość
Procesor	Intel Xeon CPU E5450, częstotliwość taktowania 3.00 GHz, 2 gniazda, 8 rdzeni, 16 procesorów logicznych
Pamięć RAM	32 GB
System operacyjny	Microsoft Windows Server 2016 Standard

Konfiguracja sprzętowa serwera SQL

Parametr	Wartość
Procesor	Intel Xeon CPU E5450, częstotliwość taktowania 3.00 GHz, 2 gniazda, 8 rdzeni, 16 procesorów logicznych
Pamięć RAM	32 GB
System operacyjny	Microsoft Windows Server 2019 Standard

Poniższa tabela wyświetla wyniki testu.

Wyniki podsumowujące testowanie działania serwera proxy KSN

Parametr	Wartość
Maksymalna liczba żądań przetworzonych na sekundę	4914
Maksymalne zużycie procesora	36%

Instalowanie Agenta sieciowego i aplikacji zabezpieczającej

Aby zarządzać urządzeniami w organizacji, na każdym z nich należy zainstalować Agenta sieciowego. Zdalna instalacja aplikacji Kaspersky Security Center na urządzeniach w firmie zazwyczaj rozpoczyna się od zainstalowania na nich Agenta sieciowego.

W systemie Microsoft Windows XP Agent sieciowy może nie wykonać poprawnie następujących działań: pobranie uaktualnień bezpośrednio z serwerów Kaspersky (jako punkt dystrybucji); działanie jako serwer proxy KSN (jako punkt dystrybucji); oraz wykrywanie luk firm trzecich (jeśli używane jest Zarządzanie lukami i poprawkami).

Wstępna zdalna instalacja

Jeśli Agent sieciowy został już zainstalowany na urządzeniu, zdalna instalacja aplikacji na tym urządzeniu odbywa się poprzez Agenta sieciowego. Pakiet dystrybucyjny aplikacji, która ma zostać zainstalowana, jest przesyłany za pośrednictwem kanałów komunikacji pomiędzy Agentami sieciowymi i Serwerem administracyjnym wraz z ustawieniami instalacji, zdefiniowanymi przez administratora. Aby przesłać pakiet dystrybucyjny, możesz użyć węzłów pośredniczących, na przykład, punktów dystrybucji, dostarczania multiemisyjnego itd. Więcej informacji dotyczących instalacji aplikacji na zarządzanych urządzeniach, na których jest już zainstalowany Agent sieciowy, można znaleźć poniżej.

Możesz przeprowadzić wstępną instalację Agenta sieciowego na urządzeniach działających pod kontrolą systemu Windows, korzystając z jednej z następujących metod:

- Używając narzędzi firm trzecich do zdalnej instalacji aplikacji.
- Klonując obraz dysku twardego administratora z systemem operacyjnym i Agentem sieciowym: przy pomocy narzędzi do zarządzania obrazami dysku, dostępnych w Kaspersky Security Center, lub przy użyciu narzędzi firm trzecich.
- Korzystając z zasad grupy w systemie Windows: używając standardowych narzędzi do zarządzania systemu Windows dla zasad grupy lub w trybie automatycznym, poprzez odpowiednią, dedykowaną opcję w zadaniu zdalnej instalacji programu Kaspersky Security Center.
- W trybie wymuszonym, korzystając ze specjalnych opcji w zadaniu zdalnej instalacji programu Kaspersky Security Center.
- Wysyłając do użytkowników urządzeń odnośniki do pakietów autonomicznych, wygenerowanych przez Kaspersky Security Center. Pakiety autonomiczne to moduły wykonywalne, które zawierają pakiety dystrybucyjne wybranych aplikacji wraz ze zdefiniowanymi ustawieniami.
- Ręcznie, poprzez uruchomienie instalatorów aplikacji na urządzeniach.

Na platformach innych niż Microsoft Windows wstępna instalacja Agenta sieciowego na zarządzanych urządzeniach musi zostać wykonana z użyciem dostępnych narzędzi firm trzecich. Na platformach innych niż Windows możesz uaktualnić Agenta sieciowego do nowej wersji lub zainstalować inne aplikacje firmy Kaspersky, korzystając z Agentów sieciowych (już zainstalowanych na urządzeniach) przeznaczonych do wykonywania zadań zdalnej instalacji. W tym przypadku instalacja przebiega identycznie jak instalacja na urządzeniach działających pod kontrolą systemu Microsoft Windows.

Podczas wybierania metody i strategii zdalnej instalacji aplikacji w zarządzanej sieci należy mieć na uwadze kilka czynników (częściowa lista):

- Konfigurację sieci organizacji.
- Całkowitą liczbę urządzeń.
- Obecność w sieci organizacji urządzeń, które nie należą do żadnej domeny Active Directory, oraz obecność jednakowych kont z uprawnieniami administratora na tych urządzeniach.
- Pojemność kanału pomiędzy Serwerem administracyjnym a urządzeniami.
- Rodzaj komunikacji pomiędzy Serwerem administracyjnym a zdalnymi podsieciami oraz pojemność kanałów sieciowych w tych podsieciach.
- Ustawienia zabezpieczeń zastosowane na zdalnych urządzeniach w momencie uruchomienia zdalnej instalacji (na przykład, użycie UAC lub Prostego udostępniania plików).

Konfigurowanie instalatorów

Przed uruchomieniem zdalnej instalacji aplikacji Kaspersky w sieci, należy określić ustawienia instalacji (ustawienia definiowane podczas instalacji aplikacji). Podczas instalacji Agenta sieciowego należy określić przynajmniej adres połączenia z Serwerem administracyjnym; niektóre ustawienia zaawansowane też mogą być wymagane. W zależności od wybranej metody instalacji, ustawienia można zdefiniować w różny sposób. W najprostszym przypadku (ręczna instalacja interaktywna na wybranym urządzeniu) wszystkie odpowiednie ustawienia można skonfigurować z poziomu interfejsu instalatora.

Ta metoda definiowania ustawień jest nieodpowiednia w nieinteraktywnej („cichej") instalacji aplikacji w grupach urządzeń. Na ogół administrator musi określić wartości dla ustawień w sposób scentralizowany; te wartości mogą być następnie użyte w instalacji nieinteraktywnej na wybranych urządzeniach w sieci.

Pakiety instalacyjne

Pierwsza i główna metoda definiowania ustawień instalacji aplikacji jest uniwersalna i tym samym jest odpowiednia dla wszystkich metod instalacji: przy użyciu narzędzi Kaspersky Security Center oraz większości narzędzi firm trzecich. Ta metoda obejmuje utworzenie pakietów instalacyjnych aplikacji w Kaspersky Security Center.

Pakiety instalacyjne są generowane przy użyciu następujących metod:

- Automatycznie, z określonych pakietów dystrybucyjnych, na podstawie załączonych *deskryptorów* (pliki z rozszerzeniem .kud, które zawierają reguły dla instalacji, wyniki analizy oraz inne informacje)
- Z plików wykonywalnych instalatorów lub z instalatorów w formacie Microsoft Windows Installer (MSI), które są dla standardowych lub obsługiwanych aplikacji

Wygenerowane pakiety instalacyjne są zorganizowane hierarchicznie jako foldery z podfolderami i plikami. Oprócz oryginalnego pakietu dystrybucyjnego, pakiet instalacyjny zawiera ustawienia dostępne do modyfikacji (w tym ustawienia instalatora oraz reguły przetwarzania dla takich sytuacji, jak konieczność ponownego uruchomienia systemu operacyjnego w celu zakończenia instalacji), a także drobne moduły pomocnicze.

Wartości ustawień instalacji, które są charakterystyczne dla pojedynczej obsługiwanej aplikacji, można zdefiniować w interfejsie Konsoli administracyjnej podczas tworzenia pakietu instalacyjnego. Podczas zdalnej instalacji aplikacji przy użyciu narzędzi Kaspersky Security Center pakiety instalacyjne są dostarczane na urządzenia, dzięki czemu uruchomienie instalatora aplikacji udostępni dla tej aplikacji wszystkie ustawienia zdefiniowane przez administratora. Jeśli do zainstalowania aplikacji firmy Kaspersky używasz narzędzi firm trzecich, musisz zapewnić dostępność całego pakietu instalacyjnego, czyli pakietu dystrybucyjnego i jego ustawień. Pakiety instalacyjne są tworzone i przechowywane przez Kaspersky Security Center w dedykowanym podfolderze folderu udostępnionego.

> W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.

Instrukcje dotyczące korzystania z tej metody konfiguracji dla aplikacji Kaspersky przed ich zainstalowaniem przy użyciu narzędzi firm trzecich można znaleźć w sekcji „Zdalna instalacja przy użyciu zasad grupy Microsoft Windows".

Natychmiast po zainstalowaniu programu Kaspersky Security Center, automatycznie zostaje wygenerowanych kilka pakietów instalacyjnych. Pakiety te są gotowe do zainstalowania i zawierają pakiety Agenta sieciowego oraz pakiety aplikacji zabezpieczających dla Microsoft Windows.

Klucz licencyjny dla aplikacji można ustawić we właściwościach pakietu instalacyjnego, jednakże zalecane jest unikanie tej metody dystrybucji licencji, gdyż w łatwy sposób można uzyskać dostęp do pakietów instalacyjnych. Dla kluczy licencyjnych należy używać zadań automatycznego rozsyłania kluczy licencyjnych lub instalacji.

Właściwości MSI i pliki transformacji

Innym sposobem skonfigurowania instalacji na platformie Windows jest zdefiniowanie właściwości MSI i plików transformacji. Ta metoda może być stosowana w następujących przypadkach:

- Podczas instalacji poprzez zasady grupy systemu Windows, korzystając ze standardowych narzędzi Microsoft lub innych narzędzi firm trzecich do zarządzania zasadami grupy systemu Windows.
- Podczas instalacji aplikacji przy użyciu narzędzi firm trzecich przeznaczonych do zarządzania instalatorami w formacie instalatora Microsoft.

Zdalna instalacja przy użyciu narzędzi firm trzecich

Jeśli w organizacji dostępne są jakiekolwiek narzędzia do zdalnej instalacji aplikacji (na przykład, Microsoft System Center), wygodnym rozwiązaniem będzie przeprowadzenie wstępnej zdalnej instalacji przy użyciu tych narzędzi.

Należy wykonać następujące czynności:

- Wybierz metodę konfiguracji instalacji, która najbardziej odpowiada używanemu narzędziu do zdalnej instalacji.
- Zdefiniuj mechanizm synchronizacji pomiędzy modyfikacją ustawień pakietów instalacyjnych (poprzez interfejs Konsoli administracyjnej) a działaniem wybranych narzędzi firm trzecich, używanych do zdalnej instalacji aplikacji z pakietu instalacyjnego.
- Podczas instalacji z folderu współdzielonego upewnij się, że ten zasób plików posiada wystarczającą pojemność.

Informacje o zadaniach zdalnej instalacji w Kaspersky Security Center

Kaspersky Security Center oferuje różne mechanizmy zdalnej instalacji aplikacji, które są zaimplementowane pod postacią zadań zdalnej instalacji (instalacja wymuszona, instalacja poprzez skopiowanie obrazu dysku twardego, instalacja poprzez zasady grupy systemu Microsoft Windows). Możesz utworzyć zadanie zdalnej instalacji dla określonej grupy administracyjnej oraz dla wskazanych urządzeń lub wyboru urządzeń (takie zadania są wyświetlane w Konsoli administracyjnej, w folderze **Zadania**). Podczas tworzenia zadania możesz wybrać pakiety instalacyjne (Agenta sieciowego i / lub innej aplikacji), które zostaną zainstalowane w obrębie tego zadania, a także określić pewne ustawienia, które definiują metodę zdalnej instalacji. Dodatkowo można użyć kreatora zdalnej instalacji, którego działanie polega na utworzeniu zadania zdalnej instalacji i monitorowaniu wyników.

Zadania dla grup administracyjnych dotyczą urządzeń znajdujących się w określonej grupie oraz wszystkich urządzeń we wszystkich podgrupach tej grupy administracyjnej. Zadanie obejmuje urządzenia podrzędnych Serwerów administracyjnych znajdujących się w grupie lub jej dowolnych podgrupach, jeśli odpowiednie ustawienie zostało włączone w zadaniu.

Zadania dla wskazanych urządzeń aktualizują listę urządzeń klienckich przy każdym uruchomieniu zgodnie z zawartością wyborów w momencie uruchomienia zadania. Jeśli wybór zawiera urządzenia, które zostały połączone z podrzędnymi Serwerami administracyjnymi, zadanie zostanie uruchomione także na tych urządzeniach. Szczegółowe informacje dotyczące tych ustawień i metod instalacji znajdują się poniżej.

Aby zapewnić pomyślne działanie zadania zdalnej instalacji na urządzeniach połączonych z podrzędnymi Serwerami administracyjnymi, należy użyć zadania przekazywania do przekazania pakietów instalacyjnych używanych przez zadanie użytkownika do odpowiednich podrzędnych Serwerów administracyjnych.

Zdalna instalacja poprzez przechwycenie i skopiowanie obrazu dysku twardego urządzenia

Jeśli konieczne jest zainstalowanie Agenta sieciowego na urządzeniach, na których musi zostać (ponownie) zainstalowany system operacyjny i inne oprogramowanie, możesz wykorzystać mechanizm przechwytywania i kopiowania obrazu dysku twardego tego urządzenia.

W celu przeprowadzenia wdrożenia poprzez przechwycenie i skopiowanie dysku twardego:

1. Utwórz urządzenie referencyjne z zainstalowanym systemem operacyjnym i niezbędnym oprogramowaniem, włączając w to Agenta sieciowego i aplikację zabezpieczającą.

2. Przechwyć obraz urządzenia referencyjnego i roześlij ten obraz na nowe urządzenia przy użyciu dedykowanego zadania z Kaspersky Security Center.

   Aby przechwytywać i instalować obrazy dysków, możesz skorzystać z narzędzi firm trzecich dostępnych w organizacji lub z funkcji (na mocy licencji Zarządzania lukami i poprawkami) oferowanej przez Kaspersky Security Center.

Jeśli do zarządzania obrazami dysków używasz narzędzi firm trzecich, podczas zdalnej instalacji na urządzeniu z obrazu referencyjnego musisz usunąć informacje, których Kaspersky Security Center używa do identyfikowania zarządzanego urządzenia. W przeciwnym razie Serwer administracyjny nie będzie mógł poprawnie odróżnić urządzeń, które zostały utworzone poprzez skopiowanie tego samego obrazu.

Podczas przechwytywania obrazu dysku przy użyciu narzędzi Kaspersky Security Center ten problem jest rozwiązywany automatycznie.

Kopiowanie dysku przy użyciu narzędzi firm trzecich

Jeśli podczas przechwytywania obrazu urządzenia z zainstalowanym Agentem sieciowym stosujesz narzędzia firm trzecich, użyj jednej z następujących metod:

- Zalecana metoda. Podczas instalacji Agenta sieciowego na urządzeniu referencyjnym, przed pierwszym uruchomieniem usługi Agenta sieciowego przechwyć obraz urządzenia (ponieważ unikatowa informacja identyfikująca urządzenie jest tworzona przy pierwszym połączeniu Agenta sieciowego z Serwerem administracyjnym). Zalecane jest unikanie uruchamiania usługi Agenta sieciowego, aż do zakończenia operacji przechwytywania obrazu.

- Na urządzeniu referencyjnym zatrzymaj usługę Agenta sieciowego i uruchom narzędzie klmover z przełącznikiem -dupfix. Narzędzie klmover znajduje się w pakiecie instalacyjnym Agenta sieciowego. Unikaj kolejnych uruchomień usługi Agenta sieciowego, dopóki operacja przechwytywania obrazu nie zostanie zakończona.

- Upewnij się, że narzędzie klmover zostanie uruchomione z przełącznikiem -dupfix przed (wymaganie obowiązkowe) pierwszym uruchomieniem usługi Agenta sieciowego na urządzeniach docelowych, przy pierwszym uruchomieniu systemu operacyjnego po zainstalowaniu obrazu. Narzędzie klmover znajduje się w pakiecie instalacyjnym Agenta sieciowego.

Jeśli obraz dysku twardego został niepoprawnie skopiowany, możesz rozwiązać ten problem.

Dla zdalnej instalacji Agenta sieciowego na nowych urządzeniach możesz zastosować alternatywny scenariusz, korzystając z obrazów systemu operacyjnego:

- Przechwycony obraz nie zawiera zainstalowanego Agenta sieciowego.
- Autonomiczny pakiet instalacyjny Agenta sieciowego, który znajduje się w folderze współdzielonym Kaspersky Security Center, został dodany do listy plików wykonywalnych uruchamianych po zakończeniu instalacji obrazu na urządzeniach docelowych.

Ten scenariusz instalacji dodaje element elastyczności: Możesz użyć jednego obrazu systemu operacyjnego z różnymi opcjami instalacji dla Agenta sieciowego i/lub aplikacji zabezpieczającej, włączając w to reguły przenoszenia urządzeń dotyczące pakietu autonomicznego. To może trochę skomplikować proces zdalnej instalacji: musisz umożliwić dostęp do folderu sieciowego z autonomicznymi pakietami instalacyjnymi z urządzenia.

Zdalna instalacja przy użyciu zasad grupy Microsoft Windows

Przeprowadzenie wstępnej instalacji Agentów sieciowych poprzez zasady grupy Microsoft Windows jest zalecane wtedy, gdy spełnione są następujące warunki:

- Urządzenie należy do domeny Active Directory.
- Schemat zdalnej instalacji umożliwia zaczekanie na kolejne rutynowe ponowne uruchomienie urządzeń docelowych przed rozpoczęciem zdalnej instalacji Agentów sieciowych na tych urządzeniach (lub można wymusić zastosowanie na tych urządzeniach zasady grupy systemu Windows).

Ten schemat instalacji charakteryzuje się następującymi cechami:

- Pakiet dystrybucyjny aplikacji w formacie Microsoft Installer (pakiet MSI) znajduje się w folderze współdzielonym (folder, w którym konta SystemLokalny urządzeń docelowych mają uprawnienia do odczytu).
- W zasadzie grupy Active Directory, dla pakietu dystrybucyjnego tworzony jest obiekt instalacji.
- Obszar instalacji jest ustawiany poprzez określenie jednostki organizacyjnej (OU) i/lub grupy zabezpieczeń, która zawiera urządzenia docelowe.
- Następnym razem, gdy urządzenie docelowe zaloguje się do domeny (przed zalogowaniem się użytkowników do systemu), wszystkie zainstalowane aplikacje są sprawdzane pod kątem żądanej aplikacji. Jeśli żądana aplikacja nie zostanie odnaleziona, pakiet dystrybucyjny zostanie pobrany z zasobu określonego w zasadzie, a następnie zostanie zainstalowany.

Ten schemat zdalnej instalacji niesie za sobą korzyść, jaką jest instalowanie przypisanych aplikacji na urządzeniach docelowych podczas ładowania systemu operacyjnego, czyli nawet przed zalogowaniem się użytkownika do systemu. Nawet jeśli użytkownik, który nie ma wystarczających uprawnień, usunie aplikację, zostanie ona ponownie zainstalowana przy kolejnym uruchomieniu systemu operacyjnego. Wadą tego schematu wdrożenia jest fakt, że zmiany w zasadzie grupowej, które zostały wprowadzone przez administratora, nie zostaną zastosowane, aż do ponownego uruchomienia urządzenia (jeśli nie są używane narzędzia dodatkowe).

Zasady grupy można użyć do zainstalowania Agenta sieciowego oraz innych aplikacji, jeśli ich instalatory są w formacie Windows Installer.

Jeśli wybierzesz ten schemat zdalnej instalacji, musisz mieć na uwadze obciążenie zasobu plików, z którego pliki zostaną skopiowane na urządzenia po zastosowaniu zasad grupy systemu Windows.

Zarządzanie zasadami Microsoft Windows przy użyciu zadania zdalnej instalacji z programu Kaspersky Security Center

Najprostszym sposobem zainstalowania aplikacji poprzez zasady grupy systemu Microsoft Windows jest zaznaczenie opcji **Przypisz pakiet instalacyjny do zasad grupy Active Directory** we właściwościach zadania zdalnej instalacji z programu Kaspersky Security Center. W tym przypadku, podczas uruchamiania zadania Serwer administracyjny automatycznie wykonuje następujące działania:

- Tworzy wymagane obiekty w zasadach grupy systemu Microsoft Windows.
- Tworzy dedykowane grupy zabezpieczeń, umieszcza w nich urządzenia docelowe i przypisuje do nich instalację wybranych aplikacji. Zbiór grup zabezpieczeń zostanie zaktualizowany przy każdym uruchomieniu zadania, zgodnie z pulą urządzeń w momencie uruchomienia.

Aby ta funkcja działała, we właściwościach zadania określ konto, które posiada uprawnienia do zapisu w zasadach grupy Active Directory.

Jeśli chcesz zainstalować Agenta sieciowego i inną aplikację przy użyciu tego samego zadania, zaznaczenie opcji **Przypisz pakiet instalacyjny do zasad grupy Active Directory** spowoduje utworzenie obiektu instalacji w zasadzie Active Directory tylko dla Agenta sieciowego. Druga aplikacja wybrana w zadaniu zostanie zainstalowana przy użyciu narzędzi Agenta sieciowego od razu po jego zainstalowaniu na urządzeniu. Jeśli poprzez zasady grupy systemu Windows chcesz zainstalować aplikację inną niż Agent sieciowy, musisz utworzyć zadanie instalacji tylko dla tego pakietu instalacyjnego (bez pakietu Agenta sieciowego). Nie każda aplikacja może zostać zainstalowana przy użyciu zasad grupy Microsoft Windows. Więcej szczegółów na temat tej możliwości można znaleźć w informacjach opisujących możliwe metody instalowania aplikacji.

Jeśli żądane obiekty są tworzone w zasadzie grupy przy użyciu narzędzi Kaspersky Security Center, folder współdzielony Kaspersky Security Center zostanie użyty jako źródło pakietu instalacyjnego. Podczas planowania zdalnej instalacji należy zestawić prędkość odczytu tego folderu z liczbą urządzeń i rozmiarem pakietu dystrybucyjnego przeznaczonego do zainstalowania. Przydatne może być umieszczenie folderu współdzielonego Kaspersky Security Center w dedykowanym repozytorium plików charakteryzującym się wysoką wydajnością.

Oprócz łatwości użycia, automatyczne tworzenie zasad grupy systemu Windows poprzez Kaspersky Security Center posiada następujące korzyści: podczas planowania instalacji Agenta sieciowego można w łatwy sposób określić grupę administracyjną Kaspersky Security Center, do której urządzenia będą automatycznie przenoszone po zakończeniu instalacji. Tę grupę można określić przy użyciu kreatora tworzenia nowego zadania lub w oknie ustawień zadania zdalnej instalacji.

Podczas zarządzania zasadami grupy systemu Windows poprzez Kaspersky Security Center możesz wskazać urządzenia dla obiektu zasad grupy, tworząc grupę zabezpieczeń. Kaspersky Security Center synchronizuje zawartość grupy zabezpieczeń z bieżącym zbiorem urządzeń uwzględnionych w zadaniu. Jeśli do zarządzania zasadami grupy używasz innych narzędzi, możesz skojarzyć obiekty zasad grupy bezpośrednio z wybranymi jednostkami organizacyjnymi Active Directory.

Samodzielna instalacja aplikacji przy użyciu zasad Microsoft Windows

Administrator może tworzyć obiekty wymagane do zainstalowania w zasadach grupy systemu Windows w swoim imieniu. W tym przypadku administrator może udostępnić odnośniki do pakietów przechowywanych w folderze współdzielonym Kaspersky Security Center lub wysłać te pakiety na dedykowany serwer plików i udostępnić odnośniki do ich pobrania.

Dostępne są następujące scenariusze instalacji:

- Administrator tworzy pakiet instalacyjny i konfiguruje jego ustawienia w Konsoli administracyjnej. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w folderze współdzielonym Kaspersky Security Center.

- Administrator tworzy pakiet instalacyjny i konfiguruje jego ustawienia w Konsoli administracyjnej. Następnie administrator kopiuje cały podfolder EXEC tego pakietu z folderu współdzielonego Kaspersky Security Center do folderu w dedykowanym zasobie plików w organizacji. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w organizacji.

- Administrator pobiera pakiet dystrybucyjny aplikacji (w tym pakiet Agenta sieciowego) z Internetu i wysyła go do dedykowanego zasobu plików w organizacji. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w organizacji. Ustawienia instalacji są definiowane poprzez konfigurowanie właściwości MSI lub poprzez konfigurowanie plików transformacji MST.

Wymuszona zdalna instalacja przy użyciu zadania zdalnej instalacji z Kaspersky Security Center

Jeśli musisz natychmiast rozpocząć instalację Agentów sieciowych lub innych aplikacji, nie czekając na zalogowanie w domenie kolejnych urządzeń docelowych, lub jeśli są dostępne jakiekolwiek urządzenia docelowe, które nie znajdują się w domenie Active Directory, możesz wymusić instalację wybranych pakietów instalacyjnych poprzez zadanie zdalnej instalacji z Kaspersky Security Center.

W tej sytuacji możesz bezpośrednio wskazać urządzenia docelowe lub wybrać grupę administracyjną Kaspersky Security Center, do której należą, bądź też utworzyć wybór urządzeń w oparciu o określone kryterium. Instalacja rozpoczyna się zgodnie z terminarzem zadania. Jeśli we właściwościach zadania włączone jest ustawienie **Uruchom pominięte zadania**, zadanie może zostać uruchomione albo natychmiast po włączeniu urządzeń docelowych, albo po ich przeniesieniu do docelowej grupy administracyjnej.

Ten rodzaj instalacji obejmuje kopiowanie plików do zasobu administracyjnego (admin$) na każdym urządzeniu oraz zdalną rejestrację usług pomocniczych na tych urządzeniach. W tym przypadku muszą być spełnione następujące warunki:

- Urządzenia muszą być dostępne dla połączenia albo po stronie Serwera administracyjnego, albo po stronie punktu dystrybucji.

- Rozwiązywanie nazw urządzeń docelowych musi działać poprawnie w sieci.

- Zasób administracyjny (admin$) musi pozostać włączony na urządzeniach docelowych.

- Na urządzeniach docelowych musi być uruchomiona usługa systemowa Serwer (domyślnie jest uruchomiona).

- W celu zezwolenia na zdalny dostęp przy użyciu narzędzi systemu Windows, na urządzeniach docelowych muszą być otwarte poniższe porty: TCP 139, TCP 445, UDP 137 i UDP 138.

- Tryb Proste udostępnianie plików musi być wyłączony na urządzeniach docelowych.

- Na urządzeniach docelowych udostępnianie i model zabezpieczeń muszą być ustawione na *Klasyczny - uwierzytelnianie użytkowników lokalnych jako samych siebie*. W żadnym wypadku nie może być ustawione *Tylko*

gość - uwierzytelnianie użytkowników lokalnych jako gościa.

- Urządzenia docelowe muszą być członkami domeny lub wcześniej należy utworzyć na urządzeniach docelowych jednakowe konta z uprawnieniami administratora.

Urządzenia w grupach roboczych mogą zostać przystosowane zgodnie z powyższymi wymaganiami przy użyciu narzędzia riprep.exe, którego opis znajduje się na stronie działu pomocy technicznej firmy Kaspersky.

Podczas instalacji na nowych urządzeniach, które jeszcze nie zostały przydzielone do żadnej grupy administracyjnej Kaspersky Security Center, możesz otworzyć właściwości zadania zdalnej instalacji i określić grupę administracyjną, do której urządzenia zostaną przeniesione po zakończeniu instalacji Agenta sieciowego.

Podczas tworzenia zadania grupowego należy pamiętać, że każde zadanie grupowe ma wpływ na wszystkie urządzenia we wszystkich grupach zagnieżdżonych w wybranej grupie. Dlatego też należy unikać powielania zadań instalacji w podgrupach.

Automatyczna instalacja jest uproszczonym sposobem tworzenia zadań dla wymuszonej instalacji aplikacji. We właściwościach grupy administracyjnej należy otworzyć listę pakietów instalacyjnych i wybrać te, które muszą zostać zainstalowane na urządzeniach w tej grupie. W rezultacie, wybrane pakiety instalacyjne zostaną automatycznie zainstalowane na wszystkich urządzeniach w tej grupie i wszystkich jej podgrupach. Przedział czasu, w trakcie którego pakiety zostaną zainstalowane, zależy od przepustowości sieci i całkowitej liczby urządzeń w sieci.

Instalacja wymuszona może być zastosowana także wtedy, gdy urządzenia nie są dostępne bezpośrednio dla Serwera administracyjnego, na przykład: urządzenia znajdują się w odizolowanych sieciach lub urządzenia są w sieci lokalnej, a Serwer administracyjny znajduje się w strefie DMZ. Aby umożliwić instalację wymuszoną, w każdej odizolowanej sieci należy umieścić punkty dystrybucji.

Korzystanie z punktów dystrybucji jako lokalnych centrów instalacji jest dobrym rozwiązaniem, gdy instalacja na urządzeniach w podsieciach komunikujących się z Serwerem administracyjnym odbywa się poprzez kanały o małej przepustowości, a pomiędzy urządzeniami w tej samej podsieci dostępny jest szeroki kanał. Jednakże należy zauważyć, że ta metoda instalacji powoduje duże obciążenie urządzeń pełniących role punktów dystrybucji. Dlatego też zalecane jest wybranie jako punktów dystrybucji mocniejszych urządzeń z jednostkami przechowywania danych o wysokim poziomie wydajności. Co więcej, wolna przestrzeń na dysku, na którym znajduje się folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit, musi wielokrotnie przekraczać całkowity rozmiar pakietów dystrybucyjnych instalowanych aplikacji.

Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center

Powyżej opisane metody wstępnej zdalnej instalacji Agenta sieciowego i innych aplikacji nie zawsze będą mogły zostać zaimplementowane, gdyż nie jest możliwe spełnienie wszystkich wymaganych warunków. W takich przypadkach można utworzyć standardowy plik wykonywalny zwany *autonomicznym pakietem instalacyjnym* poprzez Kaspersky Security Center, korzystając z pakietów instalacyjnych z odpowiednimi ustawieniami instalacji, które zostały przygotowane przez administratora. Autonomiczny pakiet instalacyjny jest przechowywany w folderze współdzielonym Kaspersky Security Center.

Korzystając z Kaspersky Security Center, możesz wysłać do wybranych użytkowników wiadomość e-mail zawierającą odnośnik do tego pliku w folderze współdzielonym oraz prośbę o jego uruchomienie (w trybie interaktywnym lub z przełącznikiem "-s" dla cichej instalacji). Do wiadomości e-mail możesz załączyć autonomiczny pakiet instalacyjny, a następnie wysłać ją do użytkowników urządzeń, którzy nie mają dostępu do folderu współdzielonego Kaspersky Security Center. Administrator może skopiować pakiet autonomiczny na nośnik wymienny, dostarczyć go na odpowiednie urządzenie, a następnie uruchomić go.

Pakiet autonomiczny można utworzyć z pakietu Agenta sieciowego, pakietu innej aplikacji (na przykład, zabezpieczającej) lub z obu pakietów. Jeśli pakiet autonomiczny został utworzony z pakietu Agenta sieciowego i innej aplikacji, instalacja rozpocznie się z Agenta sieciowego.

Podczas tworzenia pakietu autonomicznego z pakietu Agenta sieciowego możesz określić grupę administracyjną, do której nowe urządzenia (te, które nie zostały przydzielone do żadnej grup administracyjnych) zostaną automatycznie przeniesione po zakończeniu instalacji Agenta sieciowego na tych urządzeniach.

Pakiety autonomiczne mogą być uruchomione w trybie interaktywnym (opcja domyślna), wyświetlając wynik instalacji aplikacji, które zawierają, lub mogą być uruchomione w trybie cichym (z przełącznikiem "-s"). Tryb cichy może zostać użyty dla instalacji ze skryptów, na przykład, ze skryptów skonfigurowanych do uruchamiania po wdrożeniu obrazu systemu operacyjnego. Wynik instalacji w trybie cichym jest determinowany przez kod zwrotny procesu.

Opcje ręcznej instalacji aplikacji

Administratorzy lub doświadczeni użytkownicy mogą zainstalować aplikacje ręcznie w trybie interaktywnym. Mogą oni użyć oryginalnych pakietów dystrybucyjnych lub wygenerowanych z nich pakietów instalacyjnych, które są przechowywane w folderze współdzielonym Kaspersky Security Center. Domyślnie instalatory są uruchamiane w trybie interaktywnym i wyświetlają użytkownikom komunikaty z pytaniami o podanie wszystkich wymaganych wartości. Jednakże podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego z przełącznikiem "-s", instalator zostanie uruchomiony w trybie cichym i z ustawieniami, które zostały określone podczas konfiguracji pakietu instalacyjnego.

Podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego, przechowywanego w folderze współdzielonym Kaspersky Security Center, pakiet zostanie najpierw skopiowany do tymczasowego folderu lokalnego, a następnie instalator aplikacji zostanie uruchomiony z folderu lokalnego.

Zdalna instalacja aplikacji na urządzeniach z zainstalowanym Agentem sieciowym

Jeśli na urządzeniu jest zainstalowany działający Agent sieciowy, połączony z głównym Serwerem administracyjnym (lub jednym z jego Serwerów podrzędnych), możesz zaktualizować Agenta sieciowego na tym urządzeniu, a także zainstalować, zaktualizować lub usunąć dowolne obsługiwane aplikacje poprzez Agenta sieciowego.

Możesz włączyć opcję **Przy użyciu Agenta sieciowego** we właściwościach zadania zdalnej instalacji.

Jeśli ta opcja jest zaznaczona, pakiety instalacyjne z ustawieniami instalacji, zdefiniowanymi przez administratora, zostaną przesłane na urządzenia docelowe poprzez kanały komunikacyjne między Agentem sieciowym a Serwerem administracyjnym.

Aby zoptymalizować obciążenie na Serwerze administracyjnym oraz zminimalizować ruch pomiędzy Serwerem administracyjnym a urządzeniami, należy wskazać punkty dystrybucji w każdej sieci zdalnej lub domenie rozgłoszeniowej (sekcja „Informacje o punktach dystrybucji" oraz sekcja „Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji"). W tym przypadku pakiety instalacyjne oraz ustawienia instalatora są rozsyłane z Serwera administracyjnego na urządzenia docelowe poprzez punkty dystrybucji.

Co więcej, możliwe jest użycie punktów dystrybucji do transmisyjnego (multiemisja) dostarczania pakietów instalacyjnych, co pozwala znacząco zmniejszyć ruch sieciowy podczas zdalnej instalacji aplikacji.

Podczas wysyłania pakietów instalacyjnych na urządzenia docelowe poprzez kanały komunikacyjne między Agentami sieciowymi a Serwerem administracyjnym, wszystkie pakiety instalacyjne, które zostały przygotowane do wysłania, zostaną także zbuforowane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Jeśli używanych jest kilka dużych pakietów instalacyjnych różnych typów oraz wykorzystywana jest duża liczba punktów dystrybucji, rozmiar tego folderu może drastycznie się powiększyć.

Nie można ręcznie usunąć plików z folderu FTServer. Jeśli oryginalne pakiety instalacyjne zostaną usunięte, odpowiednie dane zostaną automatycznie usunięte z folderu FTServer.

Dane pobierane przez punkty dystrybucji są zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Nie można ręcznie usunąć plików z folderu $FTCITmp. Po zakończeniu działania zadań korzystających z danych z tego folderu, jego zawartość zostanie automatycznie usunięta.

Ponieważ pakiety instalacyjne są rozsyłane poprzez kanały komunikacyjne między Serwerem administracyjnym a Agentami sieciowymi z repozytorium pośredniczącego w formacie zoptymalizowanym dla transferów sieciowych, nie można wprowadzać żadnych zmian w pakietach instalacyjnych, przechowywanych w oryginalnym folderze każdego pakietu instalacyjnego. Takie zmiany nie zostałyby automatycznie zarejestrowane przez Serwer administracyjny. Jeśli chcesz ręcznie zmodyfikować pliki pakietów instalacyjnych (chociaż zalecane jest unikanie takiego rozwiązania), należy zmodyfikować dowolne ustawienia pakietu instalacyjnego w Konsoli administracyjnej. Zmodyfikowanie ustawień pakietu instalacyjnego w Konsoli administracyjnej spowoduje, że Serwer administracyjny zaktualizuje obraz pakietu w pamięci podręcznej, który został przygotowany do przesłania na urządzenia docelowe.

Zarządzanie ponownym uruchamianiem urządzeń w zadaniu zdalnej instalacji

Aby zakończyć zdalną instalację aplikacji, często wymagane jest ponowne uruchomienie urządzeń (szczególnie w systemie Windows).

Jeśli korzystasz z zadania zdalnej instalacji z Kaspersky Security Center, w Kreatorze tworzenia nowego zadania lub w oknie właściwości zadania, które zostało utworzone (**sekcja Ponowne uruchomienie systemu operacyjnego**), możesz wybrać akcję, która zostanie wykonana, gdy wymagane będzie ponowne uruchomienie:

- **Nie uruchamiaj ponownie urządzenia**. W tym przypadku komputer nie zostanie automatycznie uruchomiony ponownie. Aby zakończyć instalację, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań instalacji na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**. W tym przypadku urządzenie jest zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia instalacji. Opcja jest przydatna, gdy zadania instalacji są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**. W tym przypadku, na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Opcja **Pytaj użytkownika o akcję** jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia komputera.

Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji zabezpieczającej

Przed rozpoczęciem wdrażania ochrony należy pamiętać o możliwości aktualizacji antywirusowych baz danych (w tym modułów i łat), dostarczanych wraz z pakietem dystrybucyjnym aplikacji zabezpieczającej. Dobrym rozwiązaniem jest zaktualizowanie baz danych w pakiecie instalacyjnym aplikacji przed rozpoczęciem wdrożenia (na przykład przy użyciu odpowiedniego polecenia z menu kontekstowego wybranego pakietu instalacyjnego). Zmniejszy to liczbę ponownych uruchomień wymaganych do zakończenia wdrożenia ochrony na urządzeniach docelowych.

Korzystanie z narzędzi do zdalnej instalacji aplikacji z Kaspersky Security Center do uruchamiania odpowiednich plików wykonywalnych na zarządzanych urządzeniach

Korzystając z Kreatora tworzenia nowego pakietu, możesz wybrać dowolny plik wykonywalny i zdefiniować dla niego ustawienia wiersza poleceń. W tym celu należy dodać do pakietu instalacyjnego sam wybrany plik lub cały folder, w którym ten plik się znajduje. Następnie konieczne jest utworzenie zadania zdalnej instalacji i wybranie utworzonego pakietu instalacyjnego.

Podczas wykonywania zadania, na urządzeniach docelowych zostanie uruchomiony określony plik wykonywalny ze zdefiniowanymi ustawieniami wiersza poleceń.

Jeśli używasz instalatorów w formacie Microsoft Windows Installer (MSI), Kaspersky Security Center przeanalizuje wyniki instalacji przy użyciu standardowych narzędzi.

Jeśli dostępna jest licencja Zarządzania lukami i poprawkami, Kaspersky Security Center (podczas tworzenia pakietu instalacyjnego dla dowolnej obsługiwanej aplikacji w środowisku korporacyjnym) użyje także reguł do zainstalowania i przeanalizowania wyników instalacji, które znajdują się w jego aktualizowanej bazie danych.

W innym przypadku domyślne zadanie dla plików wykonywalnych poczeka na zakończenie uruchomionych procesów i wszystkich jego procesów podrzędnych. Po zakończeniu wszystkich uruchomionych procesów, zadanie zostanie zakończone pomyślnie niezależnie od kodu zwrotnego procesu instalacji. Aby zmienić takie zachowanie tego zadania, przed utworzeniem zadania należy ręcznie zmodyfikować pliki .kpd, które zostały wygenerowane przez Kaspersky Security Center w folderze nowo utworzonego pakietu instalacyjnego i jego podfolderach.

Aby zadanie nie czekało na zakończenie uruchomionych procesów, w sekcji [SetupProcessResult] ustaw wartość ustawienia Wait na 0:

Na przykład:
```
[SetupProcessResult]
Wait=0
```

Aby zadanie czekało tylko na zakończenie uruchomionych procesów w systemie Windows, a nie na zakończenie procesów podrzędnych, w sekcji [SetupProcessResult] ustaw wartość ustawienia WaitJob na 0, na przykład:

Na przykład:
```
[SetupProcessResult]
WaitJob=0
```

Aby zadanie zakończyło się pomyślnie lub zwróciło kod błędu w zależności od kodu zwrotnego uruchomionego procesu, w sekcji [SetupProcessResult_SuccessCodes] umieść listę pomyślnych kodów zwrotnych, na przykład:

Na przykład:
```
[SetupProcessResult_SuccessCodes]
0=
3010=
```

W tym przypadku każdy kod inny niż te znajdujące się na liście będzie zwracany jako błąd.

W celu wyświetlenia wiersza z komentarzem na temat pomyślnego zakończenia zadania lub błędu w wynikach zadania, w sekcji [SetupProcessResult_SuccessCodes] i [SetupProcessResult_ErrorCodes] wpisz krótki opis błędów odpowiadających kodom zwrotnym procesu, na przykład:

Na przykład:

[SetupProcessResult_SuccessCodes]

0= Instalacja zakończona pomyślnie

3010=Do zakończenia instalacji wymagane jest ponowne uruchomienie

[SetupProcessResult_ErrorCodes]

1602=Instalacja anulowana przez użytkownika

1603=Fatalny błąd podczas instalacji

W celu użycia narzędzi Kaspersky Security Center do zarządzania ponownym uruchomieniem urządzenia (jeśli ponowne uruchomienie jest wymagane do zakończenia działania), w sekcji [SetupProcessResult_NeedReboot] umieść listę kodów zwrotnych procesu, które wskazują na konieczność ponownego uruchomienia komputera:

Na przykład:

[SetupProcessResult_NeedReboot]

3010=

Monitorowanie zdalnej instalacji

W celu monitorowania instalacji Kaspersky Security Center oraz upewnienia się, że aplikacja zabezpieczająca i Agent sieciowy są zainstalowane na zarządzanych urządzeniach należy sprawdzić wskaźnik w sekcji **Wdrażanie**. Wskaźnik ten zlokalizowany jest w obszarze roboczym węzła Serwera administracyjnego w oknie głównym Konsoli administracyjnej. Kolory wskaźnika odzwierciedlają bieżący stan zdalnej instalacji. Obok wskaźnika wyświetlana jest liczba urządzeń, na których jest zainstalowany Agent sieciowy i aplikacje zabezpieczające. Jeśli uruchomione są jakiekolwiek zadania instalacji, postęp ich wykonania możesz monitorować w tym miejscu. Jeśli wystąpią jakiekolwiek błędy instalacyjne, liczba błędów zostanie wyświetlona w tym miejscu. Szczegóły dotyczące błędów można wyświetlić, klikając odnośnik.

Możesz także wykorzystać schemat zdalnej instalacji z obszaru roboczego folderu **Zarządzane urządzenia** na zakładce **Grupy**. Wykres odzwierciedla proces zdalnej instalacji i wyświetla liczbę urządzeń bez Agenta sieciowego, z Agentem sieciowym lub z Agentem sieciowym i aplikacją zabezpieczającą.

Więcej informacji o postępie wykonania zdalnej instalacji (lub działaniu określonego zadania instalacji) można uzyskać, otwierając okno wyników odpowiedniego zadania zdalnej instalacji: Kliknij zadanie prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wyniki**. Okno będzie wyświetlało dwie listy: górna lista zawiera stany zadania na urządzeniach, natomiast dolna lista zawiera zdarzenia zadania na urządzeniu, które jest aktualnie wybrane na górnej liście.

Informacje o błędach zdalnej instalacji zostaną dodane do dziennika zdarzeń aplikacji Kaspersky na Serwerze administracyjnym. Informacje o błędach są także dostępne w odpowiednim wyborze zdarzeń, w węźle Serwer administracyjny, na zakładce **Zdarzenia**.

Konfigurowanie instalatorów

Ta sekcja zawiera informacje na temat plików instalatorów Kaspersky Security Center i ustawień instalacji, a także zalecenia dotyczące instalacji Serwera administracyjnego i Agenta sieciowego w trybie cichym.

Informacje ogólne

Instalatory komponentów Kaspersky Security Center 14.2 (Serwer administracyjny, Agent sieciowy i Konsola administracyjna) bazują na technologii Instalatora Windows. Pakiet MSI jest podstawą instalatora. Ten format pakietów umożliwia wykorzystanie wszystkich korzyści oferowanych przez Instalator Windows: skalowalność, dostępność systemu poprawek, system transformacji, scentralizowana instalacja za pośrednictwem rozwiązań firm trzecich oraz niewidoczna rejestracja w systemie operacyjnym.

Instalacja w trybie cichym (z plikiem odpowiedzi)

Instalatory Serwera administracyjnego i Agenta sieciowego mogą pracować z plikiem odpowiedzi (ss_install.xml), w którym zintegrowane są parametry instalacji w trybie cichym bez udziału użytkownika. Plik ss_install.xml znajduje się w tym samym folderze co pakiet MSI. Jest on używany automatycznie podczas instalacji w trybie cichym. Możesz włączyć tryb cichej instalacji z użyciem przełącznika „/s" wiersza polecenia.

Na przykład:

```
setup.exe /s
```

> Przed uruchomieniem instalatora w trybie cichym przeczytaj Umowę licencyjną użytkownika końcowego (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center nie zawiera pliku TXT z treścią umowy EULA, możesz pobrać ten plik ze strony internetowej Kaspersky.

Plik ss_install.xml jest wewnętrznym formatem parametrów instalatora Kaspersky Security Center. Pakiety dystrybucyjne zawierają plik ss_install.xml z domyślnymi parametrami.

> Nie należy ręcznie modyfikować pliku ss_install.xml. Ten plik może być modyfikowany tylko przy użyciu narzędzi Kaspersky Security Center podczas edytowania parametrów pakietów instalacyjnych w Konsoli administracyjnej.

W celu zmodyfikowania pliku odpowiedzi dla instalacji Serwera administracyjnego:

1. Otwórz pakiet dystrybucyjny Kaspersky Security Center. Jeśli używasz pełnego pakietu pliku EXE, rozpakuj go.
2. Utwórz folder Serwer, otwórz wiersz polecenia, a następnie uruchom następujące polecenie:
   ```
   setup.exe /r ss_install.xml
   ```
   Plik instalacyjny Kaspersky Security Center uruchomi się.
3. Postępuj zgodnie z instrukcjami kreatora, aby skonfigurować instalację Kaspersky Security Center.

   Po zakończeniu działania kreatora plik odpowiedzi jest automatycznie modyfikowany zgodnie z nowymi ustawieniami określonymi przez użytkownika.

Instalacja Agenta sieciowego w trybie cichym (bez pliku odpowiedzi)

Agenta sieciowego można zainstalować przy użyciu jednego pakietu .msi, określając wartości właściwości MSI w standardowy sposób. Ten scenariusz umożliwia zainstalowanie Agenta sieciowego przy użyciu profili grupy. Aby uniknąć konfliktów pomiędzy parametrami zdefiniowanymi poprzez właściwości MSI a parametrami zdefiniowanymi w pliku odpowiedzi, możesz wyłączyć plik odpowiedzi, ustawiając właściwość `DONT_USE_ANSWER_FILE=1`. Poniżej znajduje się przykład uruchomienia instalatora Agenta sieciowego z pakietem .msi.

Instalacja Agenta sieciowego w trybie nieinteraktywnym wymaga akceptacji warunków Umowy licencyjnej. Użyj parametru `EULA=1` tylko wtedy, gdy w pełni przeczytałeś, zrozumiałeś i zaakceptowałeś warunki Umowy licencyjnej.

Na przykład:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Możliwe jest także zdefiniowanie parametrów instalacji dla pakietu .msi poprzez wcześniejsze przygotowanie pliku odpowiedzi (z rozszerzeniem .mst). To polecenie wygląda następująco:

Na przykład:

```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

W jednym poleceniu można określić kilka plików odpowiedzi.

Częściowa konfiguracja instalacji poprzez setup.exe

Podczas uruchamiania instalacji aplikacji z pliku setup.exe, do pakietu MSI możesz dodać wartości dowolnych właściwości MSI.

To polecenie wygląda następująco:

Na przykład:

```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parametry instalacji Serwera administracyjnego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Serwera administracyjnego. Wszystkie parametry są opcjonalne, za wyjątkiem EULA i PRIVACYPOLICY.

Parametry instalacji Serwera administracyjnego w trybie nieinteraktywnym

Właściwość MSI	Opis	Dostępne wartości
EULA	Akceptacja warunków licencji (wymagane)	• 1—W pełni przeczytałem, rozumiem i akceptuję warunki Umowy licencyjnej. • Inna wartość lub bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
PRIVACYPOLICY	Akceptacja postanowień i warunków Polityki prywatności (wymagana)	• 1—Jestem świadomy i wyrażam zgodę na przetwarzanie oraz przesyłanie moich danych (również do innych krajów) zgodnie z Polityką prywatności.

		Potwierdzam, że w pełni przeczytałem i rozumiem Politykę prywatności. • Inna wartość lub bez wartości—Nie akceptuję postanowień i warunków Polityki prywatności (instalacja nie zostanie wykonana).
INSTALLATIONMODETYPE	Typ instalacji Serwera administracyjnego	• Standardowa. • Niestandardowa.
INSTALLDIR	Folder instalacyjny aplikacji	Wartość wiersza.
ADDLOCAL	Lista komponentów przeznaczonych do zainstalowania (oddzielone przecinkami)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimalna lista komponentów wystarczających do poprawnego zainstalowania Serwera administracyjnego: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Rozmiar sieci	• NRT_1_100 — od 1 do 100 urządzeń. • NRT_100_1000 – od 101 do 1 000 urządzeń. • NRT_GREATER_1000—więcej niż 1 000 urządzeń.
SRV_ACCOUNT_TYPE	Sposób określania użytkownika dla działania usługi Serwera administracyjnego	• SrvAccountDefault—konto użytkownika zostanie utworzone automatycznie • SrvAccountUser—konto użytkownika jest określane ręcznie.
SERVERACCOUNTNAME	Nazwa użytkownika dla usługi	Wartość wiersza.
SERVERACCOUNTPWD	Hasło użytkownika dla usługi	Wartość wiersza.
DBTYPE	Typ bazy danych	• MySQL—używany będzie serwer bazy danych MySQL lub MariaDB. • MSSQL—używany będzie serwer bazy danych Microsoft SQL Server (SQL Server Express).
MYSQLSERVERNAME	Pełna nazwa serwera bazy danych MySQL lub MariaDB	Wartość wiersza.

MYSQLSERVERPORT	Numer portu używanego do nawiązania połączenia z serwerem bazy danych MySQL lub MariaDB	Wartość numeryczna.
MYSQLDBNAME	Nazwa serwera bazy danych MySQL lub MariaDB	Wartość wiersza.
MYSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z serwerem bazy danych MySQL lub MariaDB	Wartość wiersza.
MYSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z serwerem bazy danych MySQL lub MariaDB	Wartość wiersza.
MSSQLCONNECTIONTYPE	Sposób użycia bazy danych MSSQL	• InstallMSSEE—instalacja z pakietu • ChooseExisting—użycie zainstalowanego serwera.
MSSQLSERVERNAME	Pełna nazwa instancji serwera SQL	Wartość wiersza.
MSSQLDBNAME	Nazwa bazy danych serwera SQL	Wartość wiersza.
MSSQLAUTHTYPE	Metoda autoryzacji podczas nawiązywania połączenia z serwerem SQL	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z serwerem SQL w trybie SQLServer	Wartość wiersza.
MSSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z serwerem SQL w trybie SQLServer	Wartość wiersza.

CREATE_SHARE_TYPE	Metoda określania folderu współdzielonego	• Create—tworzenie nowego folderu współdzielonego; w tym przypadku należy określić następujące właściwości:
		  • SHARELOCALPATH—ścieżka dostępu do folderu lokalnego.
		  • SHAREFOLDERNAME—nazwa sieciowa folderu.
		• Null—należy określić właściwość EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Pełna ścieżka dostępu do istniejącego folderu	Wartość wiersza.

	współdzielonego	
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	Wartość numeryczna.
SERVERSSLPORT	Numer portu używanego do nawiązania bezpiecznego połączenia SSL z Serwerem administracyjnym	Wartość numeryczna.
SERVERADDRESS	Adres Serwera administracyjnego	Wartość wiersza.
SERVERCERT2048BITS	Długość klucza certyfikatu Serwera administracyjnego (bity)	• 1—długość klucza certyfikatu Serwera administracyjnego wynosi 2048 bity. • 0 — długość klucza certyfikatu Serwera administracyjnego wynosi 1024 bity. • Jeśli nie określono wartości, długość klucza certyfikatu Serwera administracyjnego wynosi 1024 bity.
MOBILESERVERADDRESS	Adres Serwera administracyjnego do nawiązywania połączenia z urządzeniami mobilnymi; ignorowane, jeśli nie wybrano komponentu MobileSupport	Wartość wiersza.

Parametry instalacji Agenta sieciowego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Agenta sieciowego. Wszystkie parametry są opcjonalne, za wyjątkiem EULA i SERVERADDRESS.

Parametry instalacji Agenta sieciowego w trybie nieinteraktywnym

Właściwość MSI	Opis	Dostępne wartości
EULA	Akceptacja postanowień i warunków Umowy licencyjnej	• 1—W pełni przeczytałem, rozumiem i akceptuję warunki Umowy licencyjnej. • 0—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana). • Bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).

DONT_USE_ANSWER_FILE	Odczyt ustawień instalacji z pliku odpowiedzi	• 1—Nie używaj. • Inna wartość lub brak wartości—Odczyt.
INSTALLDIR	Ścieżka do folderu instalacyjnego Agenta sieciowego	Wartość wiersza.
SERVERADDRESS	Adres Serwera administracyjnego (wymagane)	Wartość wiersza.
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	Wartość numeryczna.
SERVERSSLPORT	Numer portu dla szyfrowanego połączenia z Serwerem administracyjnym przy użyciu protokołu SSL	Wartość numeryczna.
USESSL	Czy użyć połączenia SSL	• 1—użyj. • Inna wartość lub brak wartości—nie używaj.
OPENUDPPORT	Czy otworzyć port UDP	• 1—otwórz. • Inna wartość lub brak wartości—nie otwieraj.
UDPPORT	Numer portu UDP	Wartość numeryczna.
USEPROXY	Czy użyć serwera proxy	• 1—użyj. • Inna wartość lub brak wartości—nie używaj.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Adres proxy i numer portu używanego do nawiązania połączenia z serwerem proxy	Wartość wiersza.
PROXYLOGIN	Konto używane do nawiązywania połączenia z serwerem proxy	Wartość wiersza.
PROXYPASSWORD	Hasło do konta dla połączenia z serwerem proxy (W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.)	Wartość wiersza.
GATEWAYMODE	Tryb użycia bramy połączenia	• 0—nie używaj bramy połączenia. • 1—użyj tego Agenta sieciowego jako bramy połączenia. • 2—połącz z Serwerem administracyjnym przy

		użyciu bramy połączenia.
GATEWAYADDRESS	Adres bramy połączenia	Wartość wiersza.
CERTSELECTION	Metoda pobierania certyfikatu	• GetOnFirstConnection—uzyskaj certyfikat z Serwera administracyjnego. • GetExistent—wybierz istniejący certyfikat. Jeśli ta opcja zostanie wybrana, należy określić właściwość CERTFILE.
CERTFILE	Ścieżka do pliku certyfikatu	Wartość wiersza.
VMVDI	Włącz tryb dynamiczny dla wirtualnej infrastruktury pulpitu Virtual Desktop Infrastructure (VDI).	• 1—włącz. • 0—nie włączaj. • Brak wartości—nie włączaj.
LAUNCHPROGRAM	Czy uruchomić usługę Agenta sieciowego po instalacji	• 1—uruchom. • Inna wartość lub brak wartości—nie uruchamiaj.
NAGENTTAGS	Znacznik dla Agenta sieciowego (ma priorytet nad znacznikiem podanym w pliku odpowiedzi)	Wartość wiersza.

Infrastruktura wirtualna

Kaspersky Security Center obsługuje użycie maszyn wirtualnych. Możesz zainstalować Agenta sieciowego i aplikację zabezpieczającą na każdej maszynie wirtualnej, a także wdrożyć ochronę maszyn wirtualnych na poziomie hipernadzorcy. W pierwszym przypadku, do ochrony maszyn wirtualnych możesz użyć standardowej aplikacji zabezpieczającej lub Kaspersky Security for Virtualization Light Agent. W drugim przypadku możesz użyć Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center obsługuje przywracanie maszyn wirtualnych do ich poprzedniego stanu.

Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych

Podczas instalacji Agenta sieciowego na maszynie wirtualnej zalecane jest rozważenie wyłączenia funkcji Kaspersky Security Center, które nie będą zbyt przydatne dla maszyn wirtualnych.

Podczas instalacji Agenta sieciowego na maszynie wirtualnej lub na szablonie przeznaczonym do wygenerowania maszyn wirtualnych, zalecane jest wykonanie następujących czynności:

- Jeśli uruchamiasz zdalną instalację, w oknie właściwości pakietu instalacyjnego Agenta sieciowego, w sekcji **Zaawansowane** zaznacz opcję **Optymalizuj ustawienia dla VDI**.
- Jeśli uruchamiasz instalację w trybie interaktywnym z udziałem kreatora, w oknie kreatora zaznacz opcję **Optymalizuj ustawienia Agenta sieciowego dla infrastruktury wirtualnej**.

Zaznaczenie tych opcji spowoduje zmianę ustawień Agenta sieciowego w taki sposób, że poniższe funkcje pozostaną domyślnie wyłączone (przed zastosowaniem zasady):

- Zbieranie informacji o zainstalowanym oprogramowaniu
- Zbieranie informacji o sprzęcie
- Zbieranie informacji o wykrytych lukach
- Zbieranie informacji o wymaganych aktualizacjach

Zazwyczaj te funkcje nie są potrzebne na maszynach wirtualnych, gdyż wykorzystują stałe oprogramowanie i sprzęt wirtualny.

Wyłączenie tych funkcji jest odwracalne. Jeśli jakakolwiek z wyłączonych funkcji jest potrzebna, możesz ją włączyć poprzez profil Agenta sieciowego lub poprzez ustawienia lokalne Agenta sieciowego. Ustawienia lokalne Agenta sieciowego są dostępne poprzez menu kontekstowe odpowiedniego urządzenia w Konsoli administracyjnej.

Obsługa dynamicznych maszyn wirtualnych

Kaspersky Security Center obsługuje dynamiczne maszyny wirtualne. Jeśli w sieci organizacji została wdrożona infrastruktura wirtualna, w pewnych przypadkach możliwe będzie korzystanie z dynamicznych (tymczasowych) maszyn wirtualnych. Dynamiczne maszyny wirtualne są tworzone pod unikatowymi nazwami w oparciu o szablony, które zostały przygotowane przez administratora. Użytkownik pracuje na maszynie wirtualnej przez jakiś czas, a następnie, po wyłączeniu maszyny zostanie ona usunięta z infrastruktury wirtualnej. Jeśli w sieci organizacji jest zainstalowany program Kaspersky Security Center, maszyna wirtualna z zainstalowanym Agentem sieciowym zostanie dodana do bazy danych Serwera administracyjnego. Po wyłączeniu maszyny wirtualnej, odpowiedni wpis musi także zostać usunięty z bazy danych Serwera administracyjnego.

Aby funkcja automatycznego usuwania wpisów na temat maszyn wirtualnych mogła działać, podczas instalacji Agenta sieciowego na szablonie dla dynamicznych maszyn wirtualnych wybierz opcję **Włącz tryb dynamiczny VDI**:

- Dla zdalnej instalacji—w oknie właściwości pakietu instalacyjnego Agenta sieciowego (sekcja **Zaawansowane**)
- Dla instalacji w trybie interaktywnym—w Kreatorze instalacji Agenta sieciowego

> Staraj się unikać zaznaczania opcji **Włącz tryb dynamiczny VDI** podczas instalacji Agenta sieciowego na urządzeniach fizycznych.

Jeśli chcesz, żeby zdarzenia z dynamicznych maszyn wirtualnych były przechowywane na Serwerze administracyjnym przez jakiś czas po usunięciu tych maszyn wirtualnych, w oknie właściwości Serwera administracyjnego, w sekcji **Repozytorium zdarzeń** wybierz opcję **Przechowuj zdarzenia po usunięciu urządzeń** i określ maksymalny czas przechowywania zdarzeń (w dniach).

Obsługa kopiowania maszyn wirtualnych

Kopiowanie maszyn wirtualnych z zainstalowanym Agentem sieciowym lub tworzenie maszyny wirtualnej z szablonu z zainstalowanym Agentem sieciowym odbywa się w ten sam sposób co zdalna instalacja Agenta sieciowego poprzez przechwycenie i skopiowanie obrazu dysku twardego. Oznacza to, że podczas kopiowania maszyn wirtualnych należy wykonać te same czynności, co podczas instalacji Agenta sieciowego poprzez skopiowanie obrazu dysku.

Jednakże dwa poniższe przypadki przedstawiają sytuacje, gdy Agent sieciowy automatycznie wykrywa kopiowanie. Dzięki temu nie ma potrzeby wykonywania wszystkich skomplikowanych działań wymienionych w sekcji "Zdalna instalacja poprzez przechwycenie i skopiowanie obrazu dysku twardego urządzenia":

- Opcja **Włącz tryb dynamiczny VDI** została wybrana po zainstalowaniu Agenta sieciowego - po każdym ponownym uruchomieniu systemu operacyjnego ta maszyna wirtualna będzie rozpoznawana jako nowe urządzenie, niezależnie od tego, czy została skopiowana.

- Używany jest jeden z następujących hipernadzorców: VMware™, HyperV® lub Xen®: Agent sieciowy wykrywa kopiowanie maszyny wirtualnej po zmienionych numerach ID sprzętu wirtualnego.

Analiza zmian w sprzęcie wirtualnym nie jest całkowicie wiarygodna. Przed szerszym zastosowaniem tej metody należy ją sprawdzić na małej puli maszyn wirtualnych dla wersji hipernadzorcy, który jest aktualnie używany w organizacji.

Obsługa przywracania systemu plików dla urządzeń z zainstalowanym Agentem sieciowym

Kaspersky Security Center jest aplikacją oferującą wiele funkcji. Przywrócenie poprzedniego stanu systemu plików na urządzeniu z zainstalowanym Agentem sieciowym doprowadzi do desynchronizacji danych i niepoprawnego działania Kaspersky Security Center.

Wycofanie systemu plików (lub jego części) może zostać wykonane w następujących przypadkach:

- Podczas kopiowania obrazu dysku twardego.

- Podczas przywracania stanu maszyny wirtualnej przy użyciu infrastruktury wirtualnej.

- Podczas przywracania danych z kopii zapasowej lub punktu odzyskiwania.

Scenariusze, w których oprogramowanie firm trzecich na urządzeniach z zainstalowanym Agentem sieciowym wpływa na zawartość folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\, są dla Kaspersky Security Center tylko krytycznymi scenariuszami. Dlatego też, jeśli to tylko możliwe, powinieneś zawsze wykluczać ten folder z procedury odzyskiwania.

Ponieważ zasady działania niektórych organizacji dopuszczają możliwość wycofania systemu plików urządzeń, obsługa wycofania systemu plików na urządzeniach z zainstalowanym Agentem sieciowym jest dostępna w Kaspersky Security Center od wersji 10 Maintenance Release 1 (Serwer administracyjny i Agenty sieciowe muszą być w wersjach 10 Maintenance Release 1 lub nowszych). Po wykryciu takich urządzeń są one automatycznie ponownie łączone z Serwerem administracyjnym z całkowitym wyczyszczeniem danych i pełną synchronizacją.

Domyślnie obsługa wykrywania wycofania systemu plików jest włączona w Kaspersky Security Center 14.2.

Jeśli jest to tylko możliwe, unikaj przywracania poprzedniego stanu folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ na urządzeniach z zainstalowanym Agentem sieciowym, gdyż całkowita ponowna synchronizacja danych zużywa dużą ilość zasobów.

Wycofanie stanu systemu jest całkowicie zabronione na urządzeniu z zainstalowanym Serwerem administracyjnym. Podobnie jest w przypadku wycofania baz danych używanych przez Serwer administracyjny.

Możesz przywrócić stan Serwera administracyjnego z kopii zapasowej tylko przy użyciu standardowego narzędzia klbackup.

Lokalna instalacja aplikacji

Sekcja ta opisuje procedurę instalacji aplikacji, które można zainstalować tylko na urządzeniach lokalnych.

Aby przeprowadzić lokalną instalację aplikacji na określonym urządzeniu klienckim, musisz mieć uprawnienia administratora na tym urządzeniu.

W celu zainstalowania aplikacji lokalnie na określonym urządzeniu klienckim:

1. Zainstaluj Agenta sieciowego na urządzeniu klienckim i skonfiguruj połączenie pomiędzy urządzeniem klienckim a Serwerem administracyjnym.
2. Zainstaluj wymagane aplikacje na urządzeniu zgodnie z opisem w dokumentacji tych aplikacji.
3. Na stacji roboczej administratora zainstaluj wtyczkę zarządzającą dla każdej z zainstalowanych aplikacji.

Kaspersky Security Center obsługuje również opcję lokalnej instalacji aplikacji przy pomocy autonomicznych pakietów instalacyjnych. Kaspersky Security Center nie obsługuje instalacji wszystkich aplikacji Kaspersky.

Lokalna instalacja Agenta sieciowego

W celu zainstalowania Agenta sieciowego lokalnie:

1. Na urządzeniu uruchom plik setup.exe z pakietu dystrybucyjnego pobranego z Internetu.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania.

2. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj tylko Agenta sieciowego Kaspersky Security Center 14.2**, aby uruchomić kreatora instalacji Agenta sieciowego. Postępuj zgodnie z instrukcjami kreatora.

   Podczas działania Kreatora instalacji możesz określić zaawansowane ustawienia Agenta sieciowego (patrz niżej).

3. Jeśli chcesz użyć swojego urządzenia jako bramy połączenia dla określonej grupy administracyjnej, w oknie **Brama połączenia** kreatora instalacji wybierz **Użyj Agenta sieciowego jako bramy połączenia w DMZ**.

4. W celu skonfigurowania Agenta sieciowego podczas instalacji na maszynie wirtualnym:

   a. Jeśli planujesz utworzyć dynamiczne maszyny wirtualne z obrazu maszyny wirtualnej, włącz tryb dynamiczny Agenta sieciowego dla Virtual Desktop Infrastructure (VDI). W tym celu, w oknie **Ustawienia zaawansowane** kreatora instalacji wybierz opcję **Włącz tryb dynamiczny VDI**.

      Pomiń ten krok, jeśli nie planujesz utworzyć dynamicznych maszyn wirtualnych z obrazu maszyny wirtualnej.

b. Zoptymalizuj działanie Agenta sieciowego dla VDI. Aby to zrobić, w oknie **Ustawienia zaawansowane** kreatora instalacji wybierz opcję **Optymalizuj ustawienia Agenta sieciowego Kaspersky Security Center dla infrastruktury wirtualnej**.

Skanowanie plików wykonywalnych w poszukiwaniu luk podczas uruchamiania urządzenia zostanie wyłączone. Spowoduje to wyłączenie wysyłania do Serwera administracyjnego informacji o następujących obiektach:

- Rejestrze sprzętu
- Aplikacje zainstalowane na urządzeniu
- Aktualizacje Microsoft Windows, które powinny zostać zainstalowane na lokalnym urządzeniu klienckim
- Luki w oprogramowaniu wykryte na lokalnym urządzeniu klienckim

Co więcej, będziesz mógł włączyć wysyłanie tych informacji we właściwościach Agenta sieciowego lub w ustawieniach profilu Agenta sieciowego.

Po zakończeniu działania kreatora instalacji, na urządzeniu zostanie zainstalowany Agent sieciowy.

Możesz wyświetlić właściwości usługi Agenta sieciowego Kaspersky Security Center; możesz także uruchamiać, zatrzymywać i monitorować aktywność Agenta sieciowego, korzystając ze standardowych narzędzi Microsoft Windows: Zarządzanie komputerem\Usługi.

Instalowanie Agenta sieciowego w trybie nieinteraktywnym (cichym)

Agent sieciowy może zostać zainstalowany w trybie nieinteraktywnym, czyli bez interaktywnego wprowadzania parametrów instalacji. W trybie nieinteraktywnej instalacji używany jest pakiet Instalatora Windows (MSI) dla Agenta sieciowego. Plik MSI znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center, w folderze Packages\NetAgent\exec.

W celu zainstalowania Agenta sieciowego na urządzeniu lokalnym w trybie nieinteraktywnym:

1. Przeczytaj Umowę licencyjną. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej.

2. Uruchom polecenie

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <parametry_instalacji>
   ```

   gdzie `setup_parameters` to lista parametrów i ich odpowiednich wartości oddzielonych spacjami (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   Na liście parametrów będziesz musiał uwzględnić `EULA=1`. W przeciwnym razie Agent sieciowy nie zostanie zainstalowany.

Jeśli używasz standardowych ustawień połączenia dla Kaspersky Security Center 11 i nowszych wersji oraz Agenta sieciowego na zdalnych urządzeniach, uruchom polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` to przełącznik do zapisywania raportów. Dziennik jest tworzony podczas instalacji Agenta sieciowego i zapisywany w C:\windows\temp\nag_inst.log.

Oprócz nag_inst.log aplikacja tworzy plik $klssinstlib.log, który zawiera dziennik instalacji. Ten plik jest przechowywany w folderze %windir%\temp lub %temp%. Do celów rozwiązywania problemów użytkownik lub specjalista z pomocy technicznej Kaspersky może potrzebować obu plików dziennika - nag_inst.log i $klssinstlib.log.

Jeśli chcesz dodatkowo określić port połączenia z Serwerem administracyjnym, uruchom polecenie:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

Parametr `SERVERPORT` odpowiada numerowi portu połączenia z Serwerem administracyjnym.

Nazwy i możliwe wartości parametrów, które mogą zostać użyte podczas instalacji Agenta sieciowego w trybie nieinteraktywnym znajdują się w sekcji Parametry instalacji Agenta sieciowego.

Instalowanie Agenta sieciowego dla systemu Linux w trybie cichym (z plikiem odpowiedzi)

Możesz zainstalować Agenta sieciowego na urządzeniach Linux przy użyciu pliku odpowiedzi—pliku tekstowego, który zawiera niestandardowy zestaw parametrów instalacji: zmienne i ich odpowiednie wartości. Korzystanie z tego pliku odpowiedzi umożliwia uruchomienie instalacji w trybie cichym (nieinteraktywnym), czyli bez udziału użytkownika.

W celu przeprowadzenia instalacji Agenta sieciowego dla systemu Linux w trybie cichym:

1. Przygotuj odpowiednie urządzenie Linux do zdalnej instalacji. Pobierz i utwórz pakiet zdalnej instalacji, używając pakietu .deb lub .rpm Agenta sieciowego, korzystając z dowolnego odpowiedniego systemu do zarządzania pakietami.

2. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

3. Przeczytaj Umowę licencyjną. Wykonaj poniższe kroki tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej.

4. Ustaw wartość zmiennej środowiskowej KLAUTOANSWERS, wprowadzając pełną nazwę pliku odpowiedzi (w tym ścieżkę dostępu), na przykład, w następujący sposób:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

5. Utwórz plik odpowiedzi (w formacie TXT) w katalogu, który określiłeś w zmiennej środowiskowej. Dodaj plik odpowiedzi do listy zmiennych w formacie VARIABLE_NAME=variable_value, każdy w oddzielnym wierszu.

   W celu poprawnego korzystania z pliku odpowiedzi, musisz umieścić go w minimalnym zestawie trzech wymaganych zmiennych:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Możesz także dodać dowolne opcjonalne zmienne, aby korzystać z bardziej określonych parametrów zdalnej instalacji. Poniższa tabela wyświetla listy zmiennych, które mogą znajdować się w pliku odpowiedzi:

   Zmienne pliku odpowiedzi użyte jako parametry instalacji Agenta sieciowego dla systemu Linux w trybie cichym

Zmienne pliku odpowiedzi użyte jako parametry instalacji Agenta sieciowego dla systemu Linux w trybie cichym

Nazwa zmiennej	Wymagane	Opis	Możliwe wartości
KLNAGENT_SERVER	Tak	Zawiera nazwę Serwera administracyjnego przedstawioną jako w pełni kwalifikowaną nazwę domeny (FQDN) lub adres IP.	Nazwa DNS lub adres IP.
KLNAGENT_AUTOINSTALL	Tak	Definiuje, czy tryb cichej (nieinteraktywnej) instalacji jest włączony.	1—Tryb cichy jest włączony; użytkownik nie zostanie zapytany o żadne działania podczas instalacji. Inna—Tryb cichy jest wyłączony; użytkownik może zostać zapytany o działania podczas instalacji.
EULA_ACCEPTED	Tak	Definiuje, czy użytkownik akceptuje Umowę licencyjną Agenta sieciowego; jeśli brakuje wartości, może być interpretowane jako brak zgody na Umowę licencyjną.	1—Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki tej Umowy licencyjnej. Inna wartość lub bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
KLNAGENT_PROXY_USE	Nie	Definiuje, czy połączenie z Serwerem administracyjnym będzie używało ustawień serwera proxy. Domyślna wartość to 0.	1—Ustawienia proxy są używane. Inna—Ustawienia proxy nie są używane.
KLNAGENT_PROXY_ADDR	Nie	Definiuje adres serwera proxy używany do nawiązania połączenia z Serwerem administracyjnym.	Nazwa DNS lub adres IP.
KLNAGENT_PROXY_LOGIN	Nie	Definiuje nazwę użytkownika użytą do zalogowania się do serwera proxy.	Dowolna istniejąca nazwa użytkownika.
KLNAGENT_PROXY_PASSWORD	Nie	Definiuje hasło użytkownika użyte do	Dowolny zestaw znaków alfanumerycznych

		zalogowania się do serwera proxy.	dozwolonych przez format hasła w systemie operacyjnym.
KLNAGENT_VM_VDI	Nie	Definiuje, czy Agent sieciowy jest zainstalowany na obrazie do utworzenia dynamicznych maszyn wirtualnych.	1—Agent sieciowy jest zainstalowany na obrazie, który jest używany jednocześnie do utworzenia dynamicznych maszyn wirtualnych. Inna—Podczas instalacji nie jest używany żaden obraz.
KLNAGENT_VM_OPTIMIZE	Nie	Definiuje, czy ustawienia Agenta sieciowego są optymalne dla hipernadzorcy.	1—Domyślne ustawienia lokalne Agenta sieciowego są modyfikowane w taki sposób, że zezwalają na zoptymalizowane użycie na hipernadzorcy.
KLNAGENT_TAGS	Nie	Wyświetla znaczniki przypisane do instancji Agenta sieciowego.	Jedna lub kilka nazw znaczników oddzielonych średnikami.
KLNAGENT_UDP_PORT	Nie	Definiuje port UDP użyty przez Agenta sieciowego. Domyślna wartość to 15000.	Dowolny istniejący numer portu.
KLNAGENT_PORT	Nie	Definiuje port nie będący TLS, użyty przez Agenta sieciowego. Domyślna wartość to 14000.	Dowolny istniejący numer portu.
KLNAGENT_SSLPORT	Nie	Definiuje port TLS, użyty przez Agenta sieciowego. Domyślna wartość to 13000.	Dowolny istniejący numer portu.
KLNAGENT_USESSL	Nie	Definiuje, czy port Transport Layer Security (TLS) jest używany do nawiązywania połączenia.	1 (domyślna)—TLS jest używany. Inna—TLS nie jest używany.
KLNAGENT_GW_MODE	Nie	Definiuje, czy brama połączenia jest używana.	1 (domyślna)—Bieżące ustawienia nie są modyfikowane (przy pierwszym połączeniu określona jest brama połączenia).

			2—Nie jest używana brama połączenia. 3—Brama połączenia jest używana. 4—Instancja Agenta sieciowego jest używana jako brama połączenia w strefie zdemilitaryzowanej (DMZ).
KLNAGENT_GW_ADDRESS	Nie	Definiuje adres bramy połączenia. Wartość jest stosowana tylko wtedy, gdy KLNAGENT_GW_MODE=3.	Nazwa DNS lub adres IP.

6. Zainstaluj agenta sieciowego:

- Aby zainstalować Agenta sieciowego z pakietu RPM w 32-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  `# rpm -i klnagent-<numer kompilacji>.i386.rpm`
- Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  `# rpm -i klnagent64-<numer kompilacji>.x86_64.rpm`
- Aby zainstalować Agenta sieciowego z pakietu RPM w 64-bitowym systemie operacyjnym dla architektury Arm, wykonaj następujące polecenie:
  `# rpm -i klnagent64-<numer kompilacji>.aarch64.rpm`
- Aby zainstalować Agenta sieciowego z pakietu DEB w 32-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  `# apt-get install ./klnagent_<numer kompilacji>_i386.deb`
- Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym, wykonaj następujące polecenie:
  `# apt-get install ./klnagent64_<numer kompilacji>_amd64.deb`
- Aby zainstalować Agenta sieciowego z pakietu DEB w 64-bitowym systemie operacyjnym dla architektury Arm, wykonaj następujące polecenie:
  `# apt-get install ./klnagent64_<numer kompilacji>_arm64.deb`

Instalacja Agenta sieciowego dla systemu Linux zostanie uruchomiona w trybie cichym; użytkownik nie zostanie zapytany o żadne działania podczas procesu.

Lokalna instalacja wtyczki zarządzającej aplikacją

W celu zainstalowania wtyczki zarządzającej aplikacją:

Na urządzeniu z zainstalowaną Konsolą administracyjną uruchom plik wykonywalny klcfginst.exe, wchodzący w skład pakietu dystrybucyjnego aplikacji.

Plik klcfginst.exe wchodzi w skład wszystkich aplikacji, którymi można zarządzać poprzez Kaspersky Security Center. Instalacja jest wykonywana przez kreator i nie wymaga ręcznej konfiguracji ustawień.

Instalowanie aplikacji w trybie nieinteraktywnym

W celu zainstalowania aplikacji w trybie nieinteraktywnym:

1. Otwórz okno główne Kaspersky Security Center.
2. W folderze **Zdalna instalacja** drzewa konsoli, w podfolderze **Pakiety instalacyjne** wybierz pakiet instalacyjny odpowiedniej aplikacji lub utwórz nowy pakiet instalacyjny dla tej aplikacji.

   Pakiet instalacyjny będzie przechowywany na Serwerze administracyjnym w folderze Pakiety, który znajduje się w folderze współdzielonym. Każdemu pakietowi instalacyjnemu odpowiada oddzielny podfolder.

3. Otwórz folder, w którym przechowywany jest żądany pakiet instalacyjny, w jeden z następujących sposobów:

   - Skopiuj folder żądanego pakietu instalacyjnego z Serwera administracyjnego na urządzenie klienckie. Następnie otwórz skopiowany folder na urządzeniu klienckim.
   - Z poziomu urządzenia klienckiego otwórz folder współdzielony na Serwerze administracyjnym, który odpowiada wymaganemu pakietowi instalacyjnemu.

   Jeśli folder współdzielony znajduje się na urządzeniu z systemem operacyjnym Microsoft Windows Vista, należy wybrać wartość **Wyłączony** dla ustawienia **Kontrola konta użytkownika: Uruchom wszystkich administratorów w trybie Zatwierdzenie administratora** (**Start** → **Panel sterowania** → **Administracja** → **Zasady zabezpieczeń lokalnych** → **Ustawienia zabezpieczeń**).

4. Następnie, w zależności od wybranej aplikacji:

   - Dla programów Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers oraz Kaspersky Security Center przejdź do podfolderu exec i przy pomocy przełącznika /s uruchom plik wykonywalny (plik z rozszerzeniem .exe).
   - Dla pozostałych aplikacji firmy Kaspersky, z otwartego folderu, przy pomocy przełącznika /s uruchom plik wykonywalny (plik z rozszerzeniem .exe).

   Uruchomienie pliku wykonywalnego z parametrami `EULA=1` i `PRIVACYPOLICY=1` oznacza, że w pełni przeczytałeś, zrozumiałeś i akceptujesz warunki Umowy licencyjnej i Polityki prywatności. Jesteś także świadomy, że Twoje dane będą zarządzane i przesyłane (w tym do innych krajów) w sposób opisany w Polityce prywatności. Treść Umowy licencyjnej i Polityki prywatności znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Akceptacja warunków Umowy licencyjnej i Polityki prywatności jest niezbędna do zainstalowania aplikacji lub jej aktualizacji z poprzedniej wersji aplikacji.

Instalowanie aplikacji przy pomocy pakietów autonomicznych

Kaspersky Security Center umożliwia utworzenie autonomicznych pakietów instalacyjnych dla aplikacji. Autonomiczny pakiet instalacyjny jest plikiem wykonywalnym, który można umieścić na serwerze sieciowym, przesłać w wiadomości e-mail lub przenieść na urządzenie klienckie w inny sposób. Możesz uruchomić odebrany plik lokalnie na urządzeniu klienckim i zainstalować aplikację bez udziału Kaspersky Security Center.

W celu zainstalowania aplikacji przy użyciu autonomicznego pakietu instalacyjnego:

1. Nawiąż połączenie z żądanym Serwerem administracyjnym.
2. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
3. W obszarze roboczym wybierz pakiet instalacyjny wymaganej aplikacji.
4. Uruchom proces tworzenia autonomicznego pakietu instalacyjnego, korzystając z jednej z następujących metod:
   - Wybierając **Utwórz autonomiczny pakiet instalacyjny** z menu kontekstowego pakietu instalacyjnego.
   - Klikając odnośnik **Utwórz autonomiczny pakiet instalacyjny** w obszarze roboczym pakietu instalacyjnego.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Postępuj zgodnie z instrukcjami kreatora.

   W ostatnim kroku kreatora wybierz metodę przesłania autonomicznego pakietu instalacyjnego na urządzenie klienckie.
5. Prześlij autonomiczny pakiet instalacyjny na urządzenie klienckie.
6. Uruchom autonomiczny pakiet instalacyjny na urządzeniu klienckim.

Aplikacja zostanie zainstalowana na urządzeniu klienckim z ustawieniami określonymi w pakiecie autonomicznym.

Po utworzeniu autonomicznego pakietu instalacyjnego, jest on automatycznie publikowany na serwerze sieciowym. Odnośnik do pobrania pakietu autonomicznego jest wyświetlany na liście utworzonych autonomicznych pakietów instalacyjnych. Jeśli to konieczne, możesz anulować publikację wybranego pakietu autonomicznego i opublikować go ponownie na serwerze sieciowym. Domyślnie, do pobrania autonomicznych pakietów instalacyjnych wykorzystywany jest port 8060.

Ustawienia pakietu instalacyjnego Agenta sieciowego

W celu skonfigurowania pakietu instalacyjnego Agenta sieciowego:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.

   Domyślnie folder **Zdalna instalacja** to podfolder folderu **Zaawansowane**.
2. Z menu kontekstowego pakietu instalacyjnego Agenta sieciowego wybierz **Właściwości**.

Zostanie otwarte okno właściwości pakietu instalacyjnego Agenta sieciowego.

Ogólne

Sekcja **Ogólny** wyświetla ogólne informacje o pakiecie instalacyjnym:

- Nazwa pakietu instalacyjnego
- Nazwę i wersję aplikacji, dla której został utworzony pakiet instalacyjny
- Rozmiar pakietu instalacyjnego
- Data utworzenia pakietu instalacyjnego

- Ścieżkę dostępu do folderu pakietu instalacyjnego

Ustawienia

Ta sekcja przedstawia ustawienia wymagane do zapewnienia właściwego działania Agenta sieciowego natychmiast po jego zainstalowaniu. Ustawienia w tej sekcji są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows.

W grupie ustawień **Folder docelowy** możesz wybrać folder na urządzeniu klienckim, w którym zostanie zainstalowany Agent sieciowy.

- **Zainstaluj w folderze domyślnym**

  Jeśli ta opcja jest zaznaczona, Agent sieciowy zostanie zainstalowany w folderze <Dysk>:\Program Files\Kaspersky Lab\NetworkAgent. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie.

  Domyślnie opcja ta jest zaznaczona.

- **Zainstaluj we wskazanym folderze**

  Jeżeli ta opcja jest zaznaczona, Agent sieciowy zostanie zainstalowany w folderze określonym w polu do wprowadzania danych.

W następującej grupie ustawień możesz określić hasło dla zadania zdalnej dezinstalacji Agenta sieciowego:

- **Użyj hasła dezinstalacyjnego**

  Jeśli ta opcja jest włączona, klikając przycisk **Modyfikuj** możesz wprowadzić hasło dezinstalacyjne (dostępne tylko dla Agenta sieciowego na urządzeniach działających pod kontrolą systemów operacyjnych Windows).

  Domyślnie opcja ta jest wyłączona.

- **Stan**

  Stan hasła: **Hasło zostało określone** lub **Hasło nie zostało określone**.

  Domyślnie hasło nie jest ustawione.

- **Chroń usługę Agenta sieciowego przed nieuprawnionym usuwaniem, zatrzymywaniem i zmianami ustawień**

  Po zainstalowaniu Agenta sieciowego na zarządzanym urządzeniu, komponent nie może zostać usunięty ani ponownie skonfigurowany bez żądanych uprawnień. Usługa Agenta sieciowego nie może zostać zatrzymana.

  Domyślnie opcja ta jest wyłączona.

- **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**

Jeśli ta opcja jest włączona, wszystkie pobrane uaktualnienia i poprawki Serwera administracyjnego, Agenta sieciowego, Konsoli administracyjnej, serwera urządzeń mobilnych Exchange oraz serwera iOS MDM zostaną zainstalowane automatycznie.

Jeśli ta opcja jest wyłączona, wszystkie pobrane uaktualnienia i poprawki zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzono*. Uaktualnienia i łaty ze stanem *Nie zdefiniowano* nie zostaną zainstalowane.

Domyślnie opcja ta jest włączona.

Połączenie

W tej sekcji możesz skonfigurować połączenie Agenta sieciowego z Serwerem administracyjnym:

W tej sekcji możesz skonfigurować połączenie Agenta sieciowego z Serwerem administracyjnym. Do nawiązania połączenia możesz użyć protokołu SSL lub UDP. W celu skonfigurowania połączenia, określ następujące ustawienia:

- **Serwer administracyjny**

  Adres urządzenia z zainstalowanym Serwerem administracyjnym.

- **Port**

  Numer portu używanego do nawiązywania połączenia.

- **Port SSL**

  Numer portu używanego do nawiązywania połączenia po protokole SSL.

- **Użyj certyfikatu Serwera**

  Jeśli ta opcja jest włączona, autoryzacja dostępu Agenta sieciowego do Serwera administracyjnego użyje pliku certyfikatu, który możesz określić, klikając przycisk **Przeglądaj**.

  Jeśli ta opcja jest wyłączona, plik certyfikatu zostanie pobrany z Serwera administracyjnego przy pierwszym połączeniu Agenta sieciowego z adresem określonym w polu **Adres serwera**.

  Nie jest zalecane wyłączenie tej opcji, ponieważ automatyczne odbieranie certyfikatu Serwera administracyjnego przez Agenta sieciowego po nawiązaniu połączenia z Serwerem administracyjnym jest uznawane z niebezpieczne.

  Domyślnie pole to jest zaznaczone.

- **Użyj SSL**

  Jeśli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

  Domyślnie opcja ta jest wyłączona. Zalecamy, aby nie wyłączać tej opcji, aby Twoje połączenie pozostało bezpieczne.

- **Użyj portu UDP**

Jeżeli ta opcja jest włączona, Agent sieciowy nawiązuje połączenie z Serwerem administracyjnym poprzez port UDP. Pozwala to na zarządzanie urządzeniami klienckimi i otrzymywanie informacji o nich.

Port UDP, który musi być otwarty na zarządzanych urządzeniach, na których jest zainstalowany Agent sieciowy. Dlatego zalecamy, aby nie wyłączać tej opcji.

Domyślnie opcja ta jest włączona.

- **Numer portu UDP**

  W tym polu możesz określić port do łączenia Agenta sieciowego z Serwerem administracyjnym przy użyciu protokołu UDP.

  Domyślny numer portu UDP to 15000.

- **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows**

  Jeżeli ta opcja jest włączona, po zainstalowaniu Agenta sieciowego na urządzeniu klienckim, port UDP zostanie dodany do listy wykluczeń Zapory systemu Microsoft Windows. Ten port UDP jest niezbędny do właściwego działania Agenta sieciowego.

  Domyślnie opcja ta jest włączona.

Zaawansowane

W sekcji **Zaawansowane** możesz skonfigurować sposób korzystania z bramy połączenia. W tym celu możesz wykonać następujące czynności:

- Użyj Agenta sieciowego jako bramy połączenia w strefie zdemilitaryzowanej (DMZ), aby połączyć się z Serwerem administracyjnym, komunikować się z nim i bezpiecznie przechowywać dane w Agencie sieciowym podczas transmisji danych.
- Połącz się z Serwerem administracyjnym przy użyciu bramy połączenia, aby zmniejszyć liczbę połączeń z Serwerem administracyjnym. W takim przypadku wprowadź adres urządzenia, które będzie pełnić funkcję bramy połączenia w polu **Adres bramy połączenia**.
- Skonfiguruj połączenie dla infrastruktury pulpitu wirtualnego (VDI), jeśli sieć obejmuje maszyny wirtualne. W tym celu wykonaj następujące czynności:
  - **Włącz tryb dynamiczny VDI**

    Jeżeli ta opcja jest włączona, tryb dynamiczny Virtual Desktop Infrastructure będzie włączony dla Agenta sieciowego, zainstalowanego na maszynie wirtualnej.

    Domyślnie opcja ta jest wyłączona.

  - **Optymalizuj ustawienia dla VDI**

Jeśli ta opcja jest włączona, w ustawieniach Agenta sieciowego będą wyłączone następujące funkcje:

- Zbieranie informacji o zainstalowanym oprogramowaniu
- Zbieranie informacji o sprzęcie
- Zbieranie informacji o wykrytych lukach
- Zbieranie informacji o wymaganych aktualizacjach

Domyślnie opcja ta jest wyłączona.

Dodatkowe składniki

W tej sekcji możesz wybrać dodatkowe komponenty do jednoczesnego zainstalowania z Agentem sieciowym.

Znaczniki

Sekcja **Znaczniki** wyświetla listę słów kluczowych (tagów), które mogą zostać dodane do urządzeń klienckich po zainstalowaniu Agenta sieciowego. Możesz dodawać i usuwać tagi do/z listy, a także zmieniać ich nazwy.

Jeśli pole obok tagu jest zaznaczone, ten tag zostanie automatycznie dodany do zarządzanych urządzeń podczas instalacji Agenta sieciowego.

Jeśli pole obok znacznika jest odznaczone, znacznik nie zostanie automatycznie dodany do zarządzanych urządzeń podczas instalacji Agenta sieciowego. Możesz ręcznie dodać ten tag do urządzeń.

Podczas usuwania tagu z listy zostanie on automatycznie usunięty ze wszystkich urządzeń, do których został dodany.

Historia rewizji

W tej sekcji możesz przejrzeć historię rewizji pakietu instalacyjnego. Możesz porównać rewizje, przejrzeć rewizje, zapisać rewizje do pliku oraz dodać i zmodyfikować opisy rewizji.

Ustawienia pakietu instalacyjnego Agenta sieciowego dostępne dla określonego systemu operacyjnego zostały podane w tabeli poniżej.

Ustawienia pakietu instalacyjnego Agenta sieciowego

Sekcja Właściwość	Windows	Mac	Linux
Ogólny	✓	✓	✓
Ustawienia	✓	–	–
Połączenie	✓	✓ (za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows** i **Używaj wyłącznie automatycznego wykrywania serwera proxy**)	✓ (za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows** i **Używaj wyłącznie automatycznego wykrywania serwera proxy**)
Zaawansowane	✓	✓	✓
Dodatkowe składniki	✓	✓	✓

Znaczniki	✓	✓ (za wyjątkiem reguł automatycznego znakowania)	✓ (za wyjątkiem reguł automatycznego znakowania)
Historia rewizji	✓	✓	✓

Przeglądanie Polityki prywatności

Polityka prywatności jest dostępna online pod adresem https://www.kaspersky.com/products-and-services-privacy-policy; jest również dostępna w trybie offline. Z Polityką prywatności możesz zapoznać się, na przykład, przed zainstalowaniem Agenta sieciowego.

W celu przeczytania Polityki prywatności w trybie offline:

1. Uruchom instalator Kaspersky Security Center.
2. W oknie instalatora przejdź do odnośnika **Wypakuj pakiety instalacyjne**.
3. Z listy, która zostanie otwarta, wybierz Agent sieciowy Kaspersky Security Center, a następnie kliknij **Dalej**.

Plik privacy_policy.txt pojawi się na Twoim urządzeniu, w określonym folderze, w podfolderze NetAgent.

Wdrażanie systemów zarządzania urządzeniami mobilnymi

Ta sekcja opisuje systemy wdrażania zarządzania urządzeniami mobilnymi poprzez protokoły Exchange ActiveSync, iOS MDM i Kaspersky Endpoint Security.

Wdrażanie systemu zarządzania poprzez protokół Exchange ActiveSync

Kaspersky Security Center umożliwia zarządzanie urządzeniami mobilnymi połączonymi z Serwerem administracyjnym przy użyciu protokołu Exchange ActiveSync. Urządzenia mobilne Exchange ActiveSync (EAS) to urządzenia połączone z serwerem urządzeń mobilnych Exchange i zarządzane przez Serwer administracyjny.

Protokół Exchange ActiveSync obsługują następujące systemy operacyjne:

- Windows Phone® 8
- Windows Phone 8.1
- Windows 10 Mobile
- Android
- iOS

Zawartość zestawu ustawień zarządzania dostępnych dla urządzenia Exchange ActiveSync zależy od systemu operacyjnego, który jest zainstalowany na urządzeniu mobilnym. Więcej informacji o funkcjach pomocniczych protokołu Exchange ActiveSync dla określonego systemu operacyjnego znajdziesz w dokumentacji załączonej do systemu operacyjnego.

Wdrażanie systemu zarządzania urządzeniami mobilnymi przy użyciu protokołu Exchange ActiveSync obejmuje następujące kroki:

1. Administrator instaluje serwer urządzeń mobilnych Exchange na wybranym urządzeniu klienckim.

2. Administrator tworzy profil(e) zarządzający w Konsoli administracyjnej do zarządzania urządzeniami EAS i dodaje ten profil(e) do skrzynek pocztowych użytkowników Exchange ActiveSync.

   Profil zarządzający urządzeń mobilnych Exchange ActiveSync jest profilem ActiveSync wykorzystywanym na serwerze Microsoft Exchange do zarządzania urządzeniami mobilnymi Exchange ActiveSync. Do skrzynki pocztowej Microsoft Exchange można przypisać tylko profil zarządzający urządzeniem EAS.

   Użytkownicy urządzeń mobilnych EAS łączą się ze swoimi skrzynkami pocztowymi Exchange. Każdy profil zarządzający nakłada ograniczenia na urządzenia mobilne.

Instalowanie serwera urządzeń mobilnych dla Exchange ActiveSync

Na urządzeniu klienckim z zainstalowanym serwerem Microsoft Exchange należy zainstalować serwer urządzeń mobilnych Exchange. Zalecane jest zainstalowanie serwera urządzeń mobilnych Exchange na serwerze Microsoft Exchange z przypisaną rolą dostępu klienta. Jeśli w tej samej domenie kilka serwerów Microsoft Exchange z przypisaną rolą Dostęp klienta tworzy macierz Dostęp klienta, zalecane jest zainstalowanie w trybie klastra serwera urządzeń mobilnych Exchange na każdym serwerze Microsoft Exchange w tej macierzy.

W celu zainstalowania serwera urządzeń mobilnych Exchange na urządzeniu lokalnym:

1. Uruchom plik wykonywalny setup.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania.

2. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj Serwer urządzeń mobilnych Exchange**, aby uruchomić kreator instalacji serwera urządzeń mobilnych Exchange.

3. W oknie **Ustawienia instalacji** wybierz typ instalacji Serwer urządzeń mobilnych Exchange:

   - Aby zainstalować serwer urządzeń mobilnych Exchange z ustawieniami domyślnymi, wybierz **Instalacja standardowa** i kliknij przycisk **Dalej**.

   - Aby ręcznie zdefiniować ustawienia instalacji serwera urządzeń mobilnych Exchange, wybierz **Instalacja niestandardowa** i kliknij **Dalej**. Następnie wykonaj poniższe czynności:

     a. W oknie **Folder docelowy** wybierz folder docelowy. Domyślny folder to <Dysk>:\Program Files\Kaspersky Lab\Mobile Device Management for Exchange. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji. Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

     b. W oknie **Tryb instalacji** wybierz typ instalacji serwera urządzeń mobilnych Exchange: tryb normalny lub tryb klastra.

     c. W oknie **Wybierz konto** wybierz konto, które będzie używane do zarządzania urządzeniami mobilnymi:

- **Utwórz konto oraz grupę ról automatycznie**. Konto zostanie utworzone automatycznie.
- **Określ konto**. Konto powinno zostać wybrane ręcznie. Kliknij przycisk **Przeglądaj**, aby wybrać konto użytkownika i określić hasło. Wybrany użytkownik powinien należeć do grupy posiadającej uprawnienia zarządzania urządzeniami mobilnymi przy użyciu ActiveSync.

d. W oknie **Ustawienia IIS** zezwól na lub zablokuj automatyczną konfigurację właściwości serwera sieciowego Internetowych usług informacyjnych (IIS).

> Jeśli zablokowałeś automatyczną konfigurację właściwości Internetowych usług informacyjnych (IIS), ręcznie włącz mechanizm „Uwierzytelniania systemu Windows" w ustawieniach IIS dla Microsoft PowerShell Virtual Directory. Jeśli mechanizm „Uwierzytelniania systemu Windows" jest wyłączony, serwer urządzeń mobilnych Exchange nie będzie działał poprawnie. Więcej informacji o konfiguracji IIS można znaleźć w dokumentacji do IIS.

e. Kliknij **Dalej**.

4. W otwartym oknie sprawdź właściwości instalacji serwera urządzeń mobilnych Exchange, a następnie kliknij **Zainstaluj**.

Po zakończeniu działania kreatora, serwer urządzeń mobilnych Exchange zostanie zainstalowany na lokalnym urządzeniu. Serwer urządzeń mobilnych Exchange będzie wyświetlany w folderze **Zarządzanie urządzeniami mobilnymi**.

Podłączanie urządzeń mobilnych do serwera urządzeń mobilnych Exchange

Przed podłączeniem jakiegokolwiek urządzenia mobilnego należy skonfigurować Microsoft Exchange Server, aby urządzenia mogły być podłączane poprzez protokół ActiveSync.

Aby podłączyć urządzenie mobilne do serwera urządzeń mobilnych Exchange, użytkownik musi połączyć się ze swoją skrzynką odbiorczą Microsoft Exchange z poziomu urządzenia mobilnego poprzez ActiveSync. Podczas łączenia użytkownik musi określić w kliencie ActiveSync ustawienia połączenia, takie jak adres e-mail oraz hasło.

Urządzenie mobilne podłączone do serwera Microsoft Exchange jest wyświetlane w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi**.

Po podłączeniu urządzenia mobilnego Exchange ActiveSync do serwera urządzeń mobilnych Exchange, administrator może zarządzać podłączonymi urządzeniami mobilnymi Exchange ActiveSync.

Konfigurowanie serwera sieciowego Internetowych usług informacyjnych

Podczas korzystania z Microsoft Exchange Server (wersji 2010 i 2013), w ustawieniach serwera sieciowego Internetowych usług informacyjnych (IIS) należy aktywować mechanizm Uwierzytelniania systemu Windows dla katalogu wirtualnego Windows PowerShell™. Ten mechanizm uwierzytelniania jest aktywowany automatycznie, jeśli w Kreatorze wdrażania serwera urządzeń mobilnych Exchange zaznaczone jest opcja **Automatycznie konfiguruj Internetowe Usługi Informacyjne Microsoft (IIS)** (jest to domyślna opcja).

W innych sytuacjach należy samodzielnie aktywować ten mechanizm uwierzytelniania.

W celu ręcznego aktywowania mechanizmu Uwierzytelniania systemu Windows dla katalogu wirtualnego PowerShell:

1. W konsoli Menedżera internetowych usług informacyjnych (IIS) otwórz właściwości katalogu wirtualnego PowerShell.

2. Przejdź do sekcji **Uwierzytelnianie**.
3. Wybierz **Uwierzytelnianie Microsoft Windows**, a następnie kliknij przycisk **Włącz**.
4. Otwórz **Ustawienia zaawansowane**.
5. Wybierz opcję **Włącz uwierzytelnianie trybu jądra**.
6. Z listy rozwijalnej **Ochrona rozszerzona** wybierz **Wymagana**.

Jeśli używany jest Microsoft Exchange Server 2007, serwer sieciowy IIS nie wymaga konfiguracji.

Lokalna instalacja serwera urządzeń mobilnych Exchange

W celu przeprowadzenia lokalnej instalacji serwera urządzeń mobilnych Exchange, administrator musi wykonać następujące działania:

1. Skopiować zawartość folderu \Server\Packages\MDM4Exchange\ z pakietu dystrybucyjnego Kaspersky Security Center na urządzenie klienckie.
2. Uruchom plik wykonywalny setup.exe.

Lokalna instalacja uwzględnia dwa typy instalacji:

- Standardowa instalacja jest uproszczoną instalacją, która nie wymaga od administratora określenia żadnych ustawień. Zalecana jest w większości przypadków.
- Rozszerzona instalacja wymaga od administratora określenia następujących ustawień:
  - Ścieżki dostępu dla instalacji serwera urządzeń mobilnych Exchange.
  - Tryb działania serwera urządzeń mobilnych Exchange: tryb standardowy lub tryb klastra.
  - Możliwość określenia konta, z poziomu którego zostanie uruchomiona usługa serwera urządzeń mobilnych Exchange.
  - Włączenie/wyłączenie automatycznej konfiguracji serwera sieciowego IIS.

Kreatora wdrażania serwera urządzeń przenośnych Exchange należy uruchomić na koncie, które ma wszystkie wymagane uprawnienia.

Zdalna instalacja serwera urządzeń mobilnych Exchange

W celu skonfigurowania zdalnej instalacji serwera urządzeń mobilnych Exchange, administrator musi wykonać następujące działania:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz folder **Zdalna instalacja**, a następnie podfolder **Pakiety instalacyjne**.
2. W podfolderze **Pakiety instalacyjne** otwórz właściwości pakietu **Wtyczka serwera urządzeń mobilnych Exchange**.
3. Przejdź do sekcji **Ustawienia**.

   Ta sekcja zawiera te same ustawienia, które są używane w lokalnej instalacji aplikacji.

Po skonfigurowaniu zdalnej instalacji, możesz uruchomić instalację serwera urządzeń mobilnych Exchange.

W celu zainstalowania serwera urządzeń mobilnych Exchange:

1. W drzewie Konsoli administracyjnej Kaspersky Security Center wybierz folder **Zdalna instalacja**, a następnie podfolder **Pakiety instalacyjne**.
2. W podfolderze **Pakiety instalacyjne** wybierz pakiet **Wtyczka serwera urządzeń mobilnych Exchange**.
3. Otwórz menu kontekstowe pakietu i wybierz **Zainstaluj aplikację**.
4. W uruchomionym kreatorze zdalnej instalacji wybierz urządzenie (lub kilka urządzeń dla instalacji w trybie klastra).
5. W polu **Uruchom Kreatora instalacji aplikacji z poziomu określonego konta** określ konto, z poziomu którego na zdalnym urządzeniu zostanie uruchomiony proces instalacji.

   Konto musi posiadać wymagane uprawnienia.

Wdrażanie systemu zarządzania poprzez protokół iOS MDM

Kaspersky Security Center umożliwia zarządzanie urządzeniami mobilnymi działającymi pod kontrolą systemu iOS. Urządzenia mobilne iOS MDM to urządzenia mobilne iOS podłączone do serwera iOS MDM i zarządzane przez Serwer administracyjny.

Podłączenie urządzeń mobilnych do serwera iOS MDM odbywa się w następujący sposób:

1. Administrator instaluje serwer iOS MDM na wybranym urządzeniu klienckim. Instalacja serwera iOS MDM jest wykonywana przy użyciu standardowych narzędzi systemu operacyjnego.
2. Administrator pobiera certyfikat Apple Push Notification Service (APNs).

   Certyfikat APN umożliwia Serwerowi administracyjnemu nawiązanie połączenia z serwerem APN w celu wysłania na urządzenia mobilne iOS MDM powiadomień wypychanych.
3. Administrator instaluje certyfikat APN na serwerze iOS MDM.
4. Administrator tworzy profil iOS MDM dla użytkownika urządzenia mobilnego iOS.

   Profil iOS MDM zawiera zbiór ustawień dotyczących łączenia urządzeń mobilnych iOS z Serwerem administracyjnym.
5. Administrator publikuje certyfikat współdzielony dla użytkownika.

   Certyfikat współdzielony jest wymagany do potwierdzenia, że urządzenie mobilne należy do użytkownika.
6. Użytkownik klika odnośnik wysłany przez administratora i pobiera pakiet instalacyjny na urządzenie mobilne.

   Pakiet instalacyjny zawiera certyfikat i profil iOS MDM.

   Po pobraniu profilu iOS MDM i zsynchronizowaniu urządzenia mobilnego iOS MDM z Serwerem administracyjnym, urządzenie zostanie wyświetlone w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli.
7. Administrator dodaje profil konfiguracyjny na serwerze iOS MDM i instaluje go na urządzeniu mobilnym po jego podłączeniu.

Profil konfiguracyjny zawiera zbiór ustawień i ograniczeń dla urządzenia mobilnego iOS MDM, na przykład ustawienia instalacji aplikacji, ustawienia użycia różnych funkcji urządzenia, ustawienia e-mail i terminarza. Profil konfiguracyjny umożliwia konfigurowanie urządzeń mobilnych iOS MDM zgodnie z polityką bezpieczeństwa firmy.

8. Jeśli jest to konieczne, administrator może dodać profile informacyjne na serwerze iOS MDM, a następnie zainstalować te profile informacyjne na urządzeniach mobilnych.

   Profil informacyjny to profil wykorzystywany do zarządzania aplikacjami rozpowszechnianymi w sposób inny niż poprzez App Store®. Profil informacyjny zawiera informacje o licencji; jest związany z określoną aplikacją.

Instalowanie serwera iOS MDM

W celu zainstalowania serwera iOS MDM na urządzeniu lokalnym:

1. Uruchom plik wykonywalny setup.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania.

   W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj serwer iOS MDM**, aby uruchomić kreator instalacji serwera iOS MDM.

2. Wybierz folder docelowy.

   Domyślny folder docelowy to <Dysk>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji. Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

3. W oknie **Określ ustawienia połączenia z serwerem iOS MDM**, w polu **Port zewnętrzny do połączenia z usługą iOS MDM** określ port zewnętrzny do łączenia urządzeń mobilnych z usługą iOS MDM.

   Port zewnętrzny 5223 jest używany przez urządzenia mobilne do komunikacji z serwerem APN. Upewnij się, że port 5223 jest otwarty w zaporze sieciowej do łączenia z zakresem adresów 17.0.0.0/8.

   Domyślnie port 443 jest używany do łączenia z serwerem iOS MDM. Jeśli port 443 jest już używany przez inną usługę lub aplikację, można go zastąpić, na przykład portem 9443.

   Serwer iOS MDM używa portu zewnętrznego 2197 do wysyłania powiadomień na serwer APN.

   Serwery APN działają w trybie równoważenia obciążenia. Urządzenia mobilne nie zawsze łączą się z tymi samymi adresami IP do pobierania powiadomień. Zakres adresów 17.0.0.0/8 jest zarezerwowany dla Apple. Dlatego też zalecane jest określenie w ustawieniach Zapory sieciowej tego całego zakresu jako dozwolonego.

4. Jeśli chcesz ręcznie skonfigurować interakcję portów dla komponentów aplikacji, wybierz opcję **Określ porty lokalne ręcznie**, a następnie określ wartości następujących ustawień:

   - **Port do połączenia z Agentem sieciowym**. W tym polu określ port dla połączenia usługi iOS MDM z Agentem sieciowym. Domyślny numer portu to 9799.
   - **Port lokalny do połączenia z usługą iOS MDM**. W tym polu określ lokalny port dla połączenia Agenta sieciowego z usługą iOS MDM. Domyślny numer portu to 9899.

   Zalecane jest użycie wartości domyślnych.

5. W oknie **Adres zewnętrzny Serwera urządzeń mobilnych**, w polu **Adres internetowy do zdalnego połączenia z Serwerem urządzeń mobilnych** określ adres urządzenia klienckiego, na którym zostanie zainstalowany serwer iOS MDM.

   Ten adres będzie używany do łączenia zarządzanych urządzeń mobilnych z usługą iOS MDM. To urządzenie klienckie powinno być dostępne dla podłączenia urządzeń iOS MDM.

Możesz określić adres urządzenia klienckiego w jednym z poniższych formatów:

- FQDN urządzenia (np. mdm.example.com)
- Nazwa NetBIOS urządzenia

W pasku adresu nie musisz dodawać numeru portu i schematu URL, ponieważ te wartości zostaną dodane automatycznie.

Po zakończeniu działania kreatora, serwer iOS MDM zostanie zainstalowany na urządzeniu lokalnym. Serwer iOS MDM będzie wyświetlany w folderze **Zarządzanie urządzeniami mobilnymi**.

Instalowanie serwera iOS MDM w trybie nieinteraktywnym

Kaspersky Security Center umożliwia zainstalowanie serwera iOS MDM na lokalnym urządzeniu klienckim w trybie nieinteraktywnym, czyli bez interaktywnego wprowadzania ustawień instalacji.

W celu zainstalowania serwera iOS MDM na urządzeniu lokalnym w trybie nieinteraktywnym:

1. Przeczytaj Umowę licencyjną. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej.
2. Uruchom następujące polecenie:
   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <parametry_instalacji>"
   ```
   gdzie `setup_parameters` to lista ustawień i ich odpowiednich wartości oddzielonych spacjami (`PRO1=PROP1VAL PROP2=PROP2VAL`). Plik setup.exe znajduje się w folderze Server, który jest częścią pakietu dystrybucyjnego Kaspersky Security Center.

Nazwy i możliwe wartości parametrów, które mogą być używane podczas instalacji serwera iOS MDM w trybie nieinteraktywnym, znajdują się w tabeli poniżej. Parametry można określać w dowolnej kolejności.

Parametry instalacji serwera iOS MDM w trybie nieinteraktywnym

Nazwa parametru	Opis parametru	Dostępne wartości
EULA	Akceptacja postanowień i warunków Umowy licencyjnej. Ten parametr jest obowiązkowy.	• 1—W pełni przeczytałem, rozumiem i akceptuję warunki Umowy licencyjnej. • Inna wartość lub bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
DONT_USE_ANSWER_FILE	Określa, czy ma być używany plik XML z ustawieniami instalacji serwera iOS MDM. Plik XML znajduje się w pakiecie instalacyjnym lub jest przechowywany na Serwerze administracyjnym. Nie ma konieczności określenia dodatkowej ścieżki do pliku. Ten parametr jest obowiązkowy.	• 1— Nie używaj pliku XML z parametrami. • Inna wartość lub brak wartości—Użyj pliku XML z parametrami.

INSTALLDIR	Folder instalacyjny serwera iOS MDM. Ten parametr jest opcjonalny.	Wartość ciągu może być, na przykład: `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	Port lokalny dla połączenia usługi iOS MDM z Agentem sieciowym. Domyślny numer portu to 9799. Ten parametr jest opcjonalny.	Wartość numeryczna.
LOCALSERVERPORT	Port lokalny dla połączenia Agenta sieciowego z usługą iOS MDM. Domyślny numer portu to 9899. Ten parametr jest opcjonalny.	Wartość numeryczna.
EXTERNALSERVERPORT	Port dla połączenia urządzenia z serwerem iOS MDM. Domyślny numer portu to 443. Ten parametr jest opcjonalny.	Wartość numeryczna.
EXTERNAL_SERVER_URL	Zewnętrzny adres urządzenia klienckiego, na którym zostanie zainstalowany serwer iOS MDM. Ten adres będzie używany do łączenia zarządzanych urządzeń mobilnych z usługą iOS MDM. To urządzenie klienckie powinno być dostępne dla podłączenia poprzez iOS MDM. Adres nie może zawierać schematu adresu URL oraz numeru portu, gdyż wartości te zostaną dodane automatycznie. Ten parametr jest opcjonalny.	• FQDN urządzenia (np. mdm.example.com) • Nazwa NetBIOS urządzenia • Adres IP urządzenia
WORKFOLDER	Folder roboczy serwera iOS MDM. Jeśli nie wskazano folderu roboczego, dane zostaną zapisane w domyślnym folderze. Ten parametr jest opcjonalny.	Wartość ciągu może być, na przykład: `WORKFOLDER=\"C:\work\"`
MTNCY	Korzystanie z serwera iOS MDM przez kilka Serwerów wirtualnych Ten parametr jest opcjonalny.	• 1—Serwer iOS MDM zostanie użyty przez kilka wirtualnych Serwerów administracyjnych. • Inna wartość lub brak wartości—Serwer iOS MDM nie zostanie użyty przez kilka wirtualnych Serwerów administracyjnych.

Na przykład:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443
EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Parametry instalacji serwera iOS MDM są opisane szczegółowo w sekcji „Instalowanie serwera iOS MDM”.

Scenariusze instalowania serwera iOS MDM

Liczba kopii serwera iOS MDM przeznaczonych do zainstalowania może zostać wybrana w oparciu o dostępny sprzęt lub całkowitą liczbę urządzeń mobilnych.

Jednakże należy pamiętać, że zalecana maksymalna liczba urządzeń mobilnych dla pojedynczej instalacji Kaspersky Device Management for iOS wynosi 50 000. Aby zmniejszyć obciążenie, cała pula urządzeń może zostać rozesłana na kilka serwerów, na których jest zainstalowany serwer iOS MDM.

Autoryzacja urządzeń iOS MDM odbywa się poprzez certyfikaty użytkownika (każdy profil zainstalowany na urządzeniu zawiera certyfikat właściciela urządzenia). Dla serwera iOS MDM dostępne są dwa schematy wdrożenia:

- Uproszczony schemat instalacji
- Schemat zdalnej instalacji z użyciem delegowania protokołu Kerberos (KCD)

Uproszczony schemat instalacji

Podczas zdalnej instalacji serwera iOS MDM z użyciem uproszczonego schematu instalacji, urządzenia mobilne łączą się bezpośrednio z usługą sieciową iOS MDM. W tym przypadku certyfikaty użytkownika wydane przez Serwer administracyjny mogą być stosowane tylko do autoryzacji urządzeń. Integracja z infrastrukturą kluczy publicznych (PKI) jest niemożliwa dla certyfikatów użytkowników.

Schemat zdalnej instalacji z użyciem delegowania protokołu Kerberos (KCD)

Schemat zdalnej instalacji z użyciem delegowania protokołu Kerberos (KCD) wymaga, aby Serwer administracyjny oraz serwer iOS MDM znajdował się w wewnętrznej sieci organizacji.

Ten schemat instalacji obejmuje:

- Integrację z Microsoft Forefront TMG
- Użycie KCD do autoryzacji urządzeń mobilnych
- Integrację z PKI do stosowania certyfikatów użytkownika

Podczas korzystania z tego schematu zdalnej instalacji należy:

- W Konsoli administracyjnej, w ustawieniach usługi sieciowej iOS MDM zaznaczyć pole **Zapewnij kompatybilność z Kerberos constrained delegation**.
- Jako certyfikat dla usługi sieciowej iOS MDM określić certyfikat niestandardowy, który został zdefiniowany, gdy usługa sieciowa iOS MDM została opublikowana na TMG.
- Certyfikaty użytkownika dla urządzeń iOS muszą być wystawione przez urząd certyfikacji (CA) domeny. Jeśli domena zawiera kilka głównych urzędów certyfikacji, certyfikaty użytkownika muszą być wystawione przez urząd certyfikacji, który został określony, gdy usługa sieciowa iOS MDM została opublikowana na TMG.

  Możesz zapewnić, że certyfikat użytkownika jest zgodny z wymaganiami wystawiania certyfikatów urzędu certyfikacji przy użyciu jednej z następujących metod:

  - Określ certyfikat użytkownika w kreatorze Nowego profilu iOS MDM oraz w kreatorze instalacji certyfikatu.

- Zintegruj Serwer administracyjny z infrastrukturą kluczy publicznych domeny oraz zdefiniuj odpowiednie ustawienie w regułach wystawiania certyfikatów:

  1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.

  2. W obszarze roboczym folderu **Certyfikaty** kliknij przycisk **Konfiguruj reguły wydawania certyfikatów**, aby otworzyć okno **Reguły wydawania certyfikatu**.

  3. W sekcji **Integracja z PKI** skonfiguruj integrację z infrastrukturą kluczy publicznych.

  4. W sekcji **Wydawanie certyfikatów dla urządzeń mobilnych** określ źródło certyfikatów.

Poniżej znajduje się przykład konfiguracji delegowania protokołu Kerberos (KCD) z następującymi założeniami:

- Usługa sieciowa iOS MDM działa na porcie 443.
- Nazwa urządzenia z TMG to tmg.mydom.local.
- Nazwa urządzenia z usługą sieciową iOS MDM to iosmdm.mydom.local.
- Nazwa zewnętrznej publikacji usługi sieciowej iOS MDM to iosmdm.mydom.global.

Nazwa główna usługi dla http/iosmdm.mydom.local

W domenie należy zarejestrować nazwę główną usługi (SPN) dla urządzenia z usługą sieciową iOS MDM (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Konfigurowanie właściwości domeny urządzenia z TMG (tmg.mydom.local)

Aby przeprowadzić ruch sieciowy, przełącz urządzenie z TMG (tmg.mydom.local) do usługi, która jest definiowana po SPN (http/iosmdm.mydom.local).

W celu przełączenia urządzenia z TMG do usługi definiowanej po SPN (http/iosmdm.mydom.local), administrator musi wykonać następujące działania:

1. W przystawce Microsoft Management Console o nazwie „Użytkownicy i komputery usługi Active Directory" wybierz urządzenie z zainstalowanym TMG (tmg.mydom.local).

2. We właściwościach urządzenia, na zakładce **Delegowanie** ustaw przełącznik **Ufaj temu komputerowi w delegowaniu tylko do określonych usług** na **Użyj dowolnego protokołu uwierzytelniania**.

3. Dodaj SPN (http/iosmdm.mydom.local) do listy **Usługi, którym to konto może przedstawiać delegowane poświadczenia**.

Specjalny (niestandardowy) certyfikat dla opublikowanej usługi sieciowej (iosmdm.mydom.global)

Konieczne jest opublikowanie specjalnego (niestandardowego) certyfikatu dla usługi sieciowej iOS MDM na FQDN iosmdm.mydom.global i określić w Konsoli administracyjnej, w ustawieniach usługi sieciowej iOS MDM, że zastępuje on domyślny certyfikat.

Należy pamiętać, że kontener certyfikatów (plik z rozszerzeniem .p12 lub .pfx) musi także zawierać łańcuch certyfikatów głównych (klucze publiczne).

Publikowanie usługi sieciowej iOS MDM na TMG

Na TMG, dla ruchu przechodzącego z urządzenia mobilnego do portu 443 usługi iosmdm.mydom.global należy skonfigurować KCD na SPN (http/iosmdm.mydom.local), korzystając z certyfikatu opublikowanego dla FQDN (iosmdm.mydom.global). Nie można zapominać, że publikacja oraz opublikowana usługa sieciowa powinny korzystać z tego samego certyfikatu serwera.

Korzystanie z serwera iOS MDM przez kilka Serwerów wirtualnych

W celu włączenia używania serwera iOS MDM przez kilka wirtualnych Serwerów administracyjnych:

1. Otwórz rejestr systemu urządzenia klienckiego, na którym jest zainstalowany serwer iOS MDM (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).
2. Przejdź do gałęzi:
   - W systemach 32-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0
   - W systemach 64-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. Dla klucza ConnectorFlags (DWORD) ustaw wartość 02102482.
4. Przejdź do gałęzi:
   - W systemach 32-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0
   - W systemach 64-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0
5. Dla klucza ConnInstalled (DWORD) ustaw wartość 00000001.
6. Uruchom ponownie usługę serwera iOS MDM.

Wartości klucza muszą być wprowadzone w określonej sekwencji.

Pobieranie certyfikatu APNs

Jeśli masz już certyfikat APNs, rozważ jego odnowienie zamiast utworzenie nowego. Po zastąpieniu istniejącego certyfikatu APNs nowo utworzonym, Serwer administracyjny utraci możliwość zarządzania aktualnie podłączonymi urządzeniami mobilnymi iOS.

Po utworzeniu Żądania podpisania certyfikatu (Certificate Signing Request - żądanie CSR) w pierwszym kroku kreatora certyfikatu APNs, jego prywatny klucz jest przechowywany w pamięci RAM Twojego urządzenia. Dlatego też wszystkie kroki kreatora muszą zostać zakończone w jednej sesji aplikacji.

W celu pobrania certyfikatu APNs:

1. W folderze **Zarządzanie urządzeniami mobilnymii** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**
2. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.
3. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera iOS MDM.
4. W oknie właściwości serwera iOS MDM wybierz sekcję **Certyfikaty**.
5. W sekcji **Certyfikaty**, w grupie ustawień **Certyfikat usługi Apple Push Notification** kliknij przycisk **Żądaj nowego**.

   Zostanie uruchomiony Kreator pobierania certyfikatu APNs i zostanie otwarte okno **Żądaj nowego**.
6. Utwórz Żądanie podpisania certyfikatu (zwane dalej CSR). W tym celu wykonaj następujące czynności:

   a. Kliknij przycisk **Utwórz CSR**.

   b. W otwartym oknie **Utwórz CSR** określ nazwę swojego żądania, nazwę firmy i oddziału, swoje miasto, region i kraj.

   c. Kliknij przycisk **Zapisz** i określ nazwę pliku, do którego zostanie zapisane Twoje żądanie CSR.

   Prywatny klucz certyfikatu zostanie zapisany w pamięci urządzenia.
7. Użyj swojego konta w serwisie CompanyAccount do wysłania pliku z CSR do Kaspersky w celu jego podpisania.

   > Podpisanie CSR będzie dostępne tylko po przesłaniu na portal CompanyAccount klucza umożliwiającego użycie funkcji Zarządzanie urządzeniami mobilnymi.

   Po przetworzeniu Twojego żądania online, otrzymasz plik CSR podpisany przez Kaspersky.
8. Wyślij podpisany plik CSR na stronę Apple Inc. przy użyciu losowego numeru Apple ID.

   > Zalecamy, aby nie używać osobistego numeru Apple ID. Utwórz dedykowany numer Apple ID, aby użyć go jako firmowego numeru ID. Po utworzeniu numeru Apple ID, skojarz go ze skrzynką pocztową firmy, a nie skrzynką pocztową pracownika.

   Po przetworzeniu Twojego żądania CSR w Apple Inc., otrzymasz publiczny klucz certyfikatu APNs. Zapisz plik na dysku.
9. Wyeksportuj certyfikat APNs wraz z prywatnym kluczem utworzonym podczas generowania żądania CSR w formacie PFX. Aby to zrobić:

   a. W oknie **Żądaj nowego certyfikatu APNs** kliknij przycisk **Zakończ CSR**.

b. W oknie **Otwórz** wybierz plik z publicznym kluczem certyfikatu, otrzymany z Apple Inc. w wyniku przetworzenia żądania CSR, a następnie kliknij przycisk **Otwórz**.

Zostanie uruchomiony proces eksportowania certyfikatu.

c. W następnym oknie wprowadź hasło prywatnego klucza i kliknij **OK**.

To hasło zostanie użyte do zainstalowania certyfikatu APN na serwerze iOS MDM.

d. W oknie **Zapisz certyfikat APNs** określ nazwę pliku dla certyfikatu APNs, wybierz folder i kliknij **Zapisz**.

Prywatne i publiczne klucze certyfikatu zostaną połączone, a certyfikat APNs zostanie zapisany w formacie PFX. Teraz możesz zainstalować certyfikat APNs na serwerze iOS MDM.

Odnawianie certyfikatu APNs

W celu odnowienia certyfikatu APNs:

1. W folderze **Zarządzanie urządzeniami mobilnymii** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**
2. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.
3. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera iOS MDM.
4. W oknie właściwości serwera iOS MDM wybierz sekcję **Certyfikaty**.
5. W sekcji **Certyfikaty**, w grupie ustawień **Certyfikat usługi Apple Push Notification** kliknij przycisk **Odnów**.

   Zostanie uruchomiony Kreator odnawiania certyfikatu usługi Apple Push Notification i zostanie otwarte okno **Odnów certyfikat APNs**.
6. Utwórz Żądanie podpisania certyfikatu (zwane dalej CSR). W tym celu wykonaj następujące czynności:

   a. Kliknij przycisk **Utwórz CSR**.

   b. W otwartym oknie **Utwórz CSR** określ nazwę swojego żądania, nazwę firmy i oddziału, swoje miasto, region i kraj.

   c. Kliknij przycisk **Zapisz** i określ nazwę pliku, do którego zostanie zapisane Twoje żądanie CSR.

   Prywatny klucz certyfikatu zostanie zapisany w pamięci urządzenia.
7. Użyj swojego konta w serwisie CompanyAccount do wysłania pliku z CSR do Kaspersky w celu jego podpisania.

   > Podpisanie CSR będzie dostępne tylko po przesłaniu na portal CompanyAccount klucza umożliwiającego użycie funkcji Zarządzanie urządzeniami mobilnymi.

   Po przetworzeniu Twojego żądania online, otrzymasz plik CSR podpisany przez Kaspersky.
8. Wyślij podpisany plik CSR na stronę Apple Inc. przy użyciu losowego numeru Apple ID.

Zalecamy, aby nie używać osobistego numeru Apple ID. Utwórz dedykowany numer Apple ID, aby użyć go jako firmowego numeru ID. Po utworzeniu numeru Apple ID, skojarz go ze skrzynką pocztową firmy, a nie skrzynką pocztową pracownika.

Po przetworzeniu Twojego żądania CSR w Apple Inc., otrzymasz publiczny klucz certyfikatu APNs. Zapisz plik na dysku.

9. Zażądaj klucza publicznego certyfikatu. W tym celu wykonaj następujące czynności:

   a. Przejdź do portalu Apple Push Certificates. Aby zalogować się w portalu, użyj identyfikatora Apple ID, otrzymanego przy pierwszym żądaniu certyfikatu.

   b. Na liście certyfikatów wybierz certyfikat, którego nazwa APSP (w formacie „APSP: <numer>") odpowiada nazwie APSP certyfikatu używanego przez serwer iOS MDM, a następnie kliknij przycisk **Odnów**.

      Certyfikat APNs zostanie odnowiony.

   c. Zapisz certyfikat utworzony na portalu.

10. Wyeksportuj certyfikat APNs wraz z prywatnym kluczem utworzonym podczas generowania żądania CSR w formacie PFX. W tym celu wykonaj następujące czynności:

    a. W oknie **Odnów certyfikat APNs** kliknij przycisk **Zakończ CSR**.

    b. W oknie **Otwórz** wybierz plik z publicznym kluczem certyfikatu, otrzymany z Apple Inc. w wyniku przetworzenia żądania CSR, a następnie kliknij przycisk **Otwórz**.

       Zostanie uruchomiony proces eksportowania certyfikatu.

    c. W następnym oknie wprowadź hasło prywatnego klucza i kliknij **OK**.

       To hasło zostanie użyte do zainstalowania certyfikatu APN na serwerze iOS MDM.

    d. W otwartym oknie **Odnów certyfikat APNs** określ nazwę pliku dla certyfikatu APNs, wybierz folder i kliknij **Zapisz**.

Prywatne i publiczne klucze certyfikatu zostaną połączone, a certyfikat APNs zostanie zapisany w formacie PFX.

Konfigurowanie zapasowego certyfikatu serwera iOS MDM

Funkcjonalność serwera iOS MDM umożliwia wystawienie certyfikatu zapasowego. Ten certyfikat jest przeznaczony do użycia w profilach iOS MDM, aby zapewnić bezproblemowe przełączanie zarządzanych urządzeń iOS po wygaśnięciu certyfikatu iOS MDM Server.

Jeśli Twój serwer iOS MDM używa domyślnego certyfikatu wystawionego przez Kaspersky, możesz wystawić certyfikat zapasowy (lub określić własny certyfikat niestandardowy jako zapasowy) przed wygaśnięciem certyfikatu serwera iOS MDM. Domyślnie certyfikat zapasowy jest wystawiany automatycznie 60 dni przed wygaśnięciem certyfikatu serwera iOS MDM. Zapasowy certyfikat serwera iOS MDM staje się certyfikatem głównym natychmiast po wygaśnięciu certyfikatu serwera iOS MDM. Klucz publiczny jest dystrybuowany do wszystkich zarządzanych urządzeń za pośrednictwem profili konfiguracyjnych, więc nie ma konieczności ręcznego przesyłania go.

W celu wystawienia certyfikatu zapasowego serwera iOS MDM lub określenia niestandardowego certyfikatu zapasowego:

1. W drzewie konsoli, w folderze **Zarządzanie urządzeniami mobilnymi** wybierz podfolder **Serwery urządzeń mobilnych**.

2. Na liście serwerów urządzeń mobilnych wybierz odpowiedni serwer iOS MDM, a następnie w prawej części okna kliknij przycisk **Konfiguruj Serwer iOS MDM**.

3. W oknie ustawień serwera iOS MDM wybierz sekcję **Certyfikaty**.

4. W sekcji ustawień **Certyfikat zapasowy** wykonaj jedną z następujących czynności:

   - Jeśli planujesz nadal korzystać z certyfikatu z podpisem własnym (czyli certyfikatu wystawionego przez Kaspersky):

     a. Kliknij przycisk **Wydanie**.

     b. W oknie **Data aktywacji**, które zostanie otwarte, wybierz jedną z dwóch opcji daty, kiedy należy zastosować certyfikat zapasowy:

        - Jeśli chcesz zastosować certyfikat zapasowy w momencie wygaśnięcia aktualnego certyfikatu, wybierz opcję **Kiedy aktualny certyfikat wygaśnie**.

        - Jeśli chcesz zastosować certyfikat zapasowy przed wygaśnięciem bieżącego certyfikatu, wybierz opcję **Po określonym czasie (w dniach)**. W polu wejściowym obok tej opcji określ czas, po upływie którego certyfikat zapasowy musi zastąpić aktualny certyfikat.

        > Okres ważności certyfikatu zapasowego, który określisz, nie może przekraczać okresu ważności bieżącego certyfikatu serwera iOS MDM.

     c. Kliknij przycisk **OK**.

     Zostanie utworzony zapasowy certyfikat serwera iOS MDM.

   - Jeśli planujesz używać niestandardowego certyfikatu wydanego przez urząd certyfikacji:

     a. Kliknij przycisk **Dodaj**.

     b. W otwartym oknie Eksploratora plików określ plik certyfikatu w formacie PEM, PFX lub P12 który jest przechowywany na urządzeniu, a następnie kliknij przycisk **Otwórz**.

     Twój niestandardowy certyfikat jest określony jako zapasowy certyfikat serwera iOS MDM.

Masz określony zapasowy certyfikat serwera iOS MDM. Szczegóły certyfikatu zapasowego są wyświetlane w sekcji ustawień **Certyfikat zapasowy** (nazwa certyfikatu, nazwa wystawcy, data wygaśnięcia i data zastosowania certyfikatu zapasowego, jeśli istnieje).

Instalowanie certyfikatu APNs na serwerze iOS MDM

Po otrzymaniu certyfikatu APNs, powinieneś zainstalować go na serwerze iOS MDM.

W celu zainstalowania certyfikatu APNs na serwerze iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**

2. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.

3. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera iOS MDM.

4. W oknie właściwości serwera iOS MDM wybierz sekcję **Certyfikaty**.

W sekcji **Certyfikaty**, w grupie ustawień **Certyfikat usługi Apple Push Notification** kliknij przycisk **Zainstaluj**.

1. Wybierz plik PFX, który zawiera certyfikat APN.

2. Wprowadź hasło klucza prywatnego, które zostało określone podczas eksportowania certyfikatu APNs.

Certyfikat APNs zostanie zainstalowany na serwerze iOS MDM. Szczegóły dotyczące certyfikatu będą wyświetlane w oknie właściwości serwera iOS MDM, w sekcji **Certyfikaty**.

Konfigurowanie dostępu do usługi Apple Push Notification

W celu zapewnienia poprawnego działania usługi sieciowej iOS MDM oraz reakcji urządzeń w odpowiednim momencie na polecenia administratora, w ustawieniach serwera iOS MDM należy określić certyfikat Apple Push Notification Service (zwany dalej certyfikatem APNs).

Podczas interakcji z Apple Push Notification (zwane dalej APNs) usługa sieciowa iOS MDM łączy się z zewnętrznym adresem api.push.apple.com poprzez port 2197 (wychodzący). Dlatego też, usługa sieciowa iOS MDM wymaga dostępu do portu TCP 2197 dla zakresu adresów 17.0.0.0/8. Ze strony urządzenia iOS możliwy jest dostęp do portu TCP 5223 dla zakresu adresów 17.0.0.0/8.

Jeśli chcesz uzyskać dostęp do APN ze strony usługi sieciowej iOS MDM poprzez serwer proxy, na urządzeniu z zainstalowaną usługą sieciową iOS MDM musisz wykonać następujące działania:

1. Dodaj do rejestru następujące wiersze:

   - W 32-bitowych systemach operacyjnych:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cons
"ApnProxyHost"="<Nazwa Hosta Proxy>"
"ApnProxyPort"="<Port Proxy>"
"ApnProxyLogin"="<Login Proxy>"
"ApnProxyPwd"="<Hasło Proxy>"
```

   - W 64-bitowych systemach operacyjnych:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSM
"ApnProxyHost"="<Nazwa Hosta Proxy>"
"ApnProxyPort"="<Port Proxy>"
"ApnProxyLogin"="<Login Proxy>"
"ApnProxyPwd"="<Hasło Proxy>"
```

2. Uruchom ponownie usługę sieciową iOS MDM.

Publikowanie i instalowanie certyfikatu współdzielonego na urządzeniu mobilnym

W celu opublikowania certyfikatu współdzielonego dla użytkownika:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz konto użytkownika.
2. Z menu kontekstowego konta użytkownika wybierz **Zainstaluj certyfikat**.

   Zostanie uruchomiony kreator instalacji certyfikatu. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora certyfikat zostanie utworzony i dodany do listy certyfikatów użytkownika.

Wydany certyfikat zostanie pobrany przez użytkownika wraz z pakietem instalacyjnym zawierającym profil iOS MDM.

Po podłączeniu urządzenia mobilnego do serwera iOS MDM, ustawienia profilu iOS MDM zostaną zastosowane na urządzeniu użytkownika. Administrator będzie mógł zarządzać urządzeniem po jego podłączeniu.

Urządzenie mobilne użytkownika podłączone do serwera iOS MDM jest wyświetlane w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi**.

Dodawanie urządzeń KES do listy zarządzanych urządzeń

W celu dodania urządzenia KES do listy zarządzanych urządzeń przy użyciu odnośnika do sklepu Google Play™:

1. Z drzewa konsoli wybierz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.
2. Wybierz konto użytkownika, którego urządzenie mobilne chcesz dodać do listy zarządzanych urządzeń.
3. W menu kontekstowym konta użytkownika wybierz **Dodaj urządzenie mobilne**.

   Zostanie uruchomiony kreator podłączania urządzenia mobilnego. W oknie **Źródło certyfikatu** musisz określić metodę tworzenia współdzielonego certyfikatu, którego Serwer administracyjny użyje do identyfikacji urządzenia mobilnego. Certyfikat współdzielony można określić na jeden z następujących sposobów:

   - Automatycznie utwórz certyfikat współdzielony przy użyciu narzędzi Serwera administracyjnego, a następnie wyślij certyfikat na urządzenie.
   - Wskaż plik współdzielonego certyfikatu.
4. W oknie **Typ urządzenia** wybierz **Odnośnik do Google Play**.
5. W oknie **Metoda powiadamiania użytkownika** zdefiniuj ustawienia powiadamiania użytkownika urządzenia mobilnego o utworzeniu certyfikatu (za pośrednictwem wiadomości SMS, poczty elektronicznej lub poprzez wyświetlenie informacji po zakończeniu działania kreatora).
6. W oknie z informacjami o certyfikacie kliknij przycisk **Zakończ**, aby zakończyć działanie kreatora.

Po zakończeniu działania kreatora, odnośnik oraz kod QR zostaną wysłane na urządzenie mobilne użytkownika, umożliwiając mu w ten sposób pobranie Kaspersky Endpoint Security ze sklepu Google Play. Użytkownik otwiera stronę sklepu Google Play poprzez kliknięcie odsyłacza lub przeskanowanie kodu QR. System operacyjny urządzenia wyświetla pytanie o zaakceptowanie instalacji Kaspersky Endpoint Security for Android. Po pobraniu i zainstalowaniu Kaspersky Endpoint Security for Android, urządzenie mobilne nawiązuje połączenie z Serwerem administracyjnym i pobiera współdzielony certyfikat. Po zainstalowaniu certyfikatu na urządzeniu mobilnym, urządzenie zostanie wyświetlone w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli.

Jeśli program Kaspersky Endpoint Security for Android jest już zainstalowany na urządzeniu, użytkownik musi otrzymać ustawienia połączenia z Serwerem Administracyjnym od administratora, a następnie samodzielnie wprowadzić je na urządzeniu. Po zdefiniowaniu ustawień połączenia, urządzenie mobilne łączy się z Serwerem Administracyjnym. Administrator wystawia certyfikat współdzielony dla urządzenia i wysyła użytkownikowi wiadomość e-mail lub wiadomość SMS z nazwą użytkownika i hasłem do pobrania certyfikatu. Użytkownik pobiera i instaluje współdzielony certyfikat. Po zainstalowaniu certyfikatu na urządzeniu mobilnym, urządzenie zostanie wyświetlone w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli. W tym przypadku program Kaspersky Endpoint Security for Android nie zostanie pobrany i ponownie zainstalowany.

Połączenie urządzeń KES z Serwerem administracyjnym

W zależności od metody używanej do łączenia urządzeń z Serwerem administracyjnym, dla Kaspersky Device Management for iOS istnieją dwa schematy zdalnej instalacji na urządzeniach KES:

- Schemat zdalnej instalacji z bezpośrednim połączeniem urządzeń z Serwerem administracyjnym
- Schemat zdalnej instalacji uwzględniający Forefront® Threat Management Gateway (TMG)

Bezpośrednie połączenie urządzeń z Serwerem administracyjnym

Urządzenia KES mogą łączyć się bezpośrednio z portem 13292 Serwera administracyjnego.

W zależności od metody używanej do autoryzacji, dla połączenia urządzeń KES z Serwerem administracyjnym możliwe są dwie opcje:

- Łączenie urządzeń z użyciem certyfikatu użytkownika
- Łączenie urządzeń bez użycia certyfikatu użytkownika

Łączenie urządzeń z użyciem certyfikatu użytkownika

Podczas łączenia urządzeń z użyciem certyfikatu użytkownika, to urządzenie jest kojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

W tym przypadku używane będzie dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne). Serwer administracyjny i urządzenie będą uwierzytelniani przy użyciu certyfikatów.

Łączenie urządzeń bez użycia certyfikatu użytkownika

Podczas łączenia urządzenia bez użycia certyfikatu użytkownika, to urządzenie nie jest kojarzone z żadnym kontem użytkownika na Serwerze administracyjnym. Jednakże, gdy urządzenie pobierze dowolny certyfikat, to urządzenie zostanie skojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

Podczas łączenia tego urządzenia z Serwerem administracyjnym zostanie zastosowane jednokierunkowe uwierzytelnianie SSL, co oznacza, że tylko Serwer administracyjny będzie uwierzytelniony przy użyciu certyfikatu. Po pobraniu przez urządzenie certyfikatu użytkownika, typ autoryzacji zmieni się na dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne).

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD)

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD) uwzględnia:

- Integrację z Microsoft Forefront TMG.
- Użycie delegowania protokołu Kerberos (zwane również KCD) do uwierzytelnia urządzeń mobilnych.
- Integrację z infrastrukturą kluczy publicznych (zwana również PKI) w celu zastosowania certyfikatów użytkownika.

Podczas korzystania z tego schematu połączenia należy pamiętać, że:

- Typem połączenia urządzeń KES z TMG ma być "dwukierunkowe uwierzytelnianie SSL", czyli urządzenie musi łączyć się z TMG poprzez swój własny certyfikat użytkownika. W tym celu należy zintegrować certyfikat użytkownika z pakietem instalacyjnym programu Kaspersky Endpoint Security for Android, który został zainstalowany na urządzeniu. Ten pakiet KES musi być utworzony przez Serwer administracyjny specjalnie dla tego urządzenia (użytkownika).
- Dla protokołu mobilnego powinieneś określić specjalny (niestandardowy) certyfikat zamiast domyślnego certyfikatu serwera:

  1. W oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat**.
  2. W otwartym oknie określ ten sam certyfikat, który został ustawiony na TMG, gdy punkt dostępu do protokołu mobilnego został opublikowany na Serwerze administracyjnym.

- Certyfikaty użytkownika dla urządzeń KES muszą być wystawione przez urząd certyfikacji (CA) domeny. Należy pamiętać, że jeśli domena zawiera kilka głównych urzędów certyfikacji, certyfikaty użytkownika muszą być wystawione przez urząd certyfikacji, który został ustawiony w publikacji na TMG.

  Możesz upewnić się, że certyfikat użytkownika jest zgodny z wyżej opisanymi wymaganiami przy użyciu jednej z następujących metod:

  - Określ specjalny certyfikat użytkownika w kreatorze Nowego pakietu oraz kreatorze instalacji Certyfikatu.
  - Zintegruj Serwer administracyjny z infrastrukturą kluczy publicznych domeny oraz zdefiniuj odpowiednie ustawienie w regułach wystawiania certyfikatów:

    1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.
    2. W obszarze roboczym folderu **Certyfikaty** kliknij przycisk **Konfiguruj reguły wydawania certyfikatów**, aby otworzyć okno **Reguły wydawania certyfikatu**.

3. W sekcji **Integracja z PKI** skonfiguruj integrację z infrastrukturą kluczy publicznych.

4. W sekcji **Wydawanie certyfikatów dla urządzeń mobilnych** określ źródło certyfikatów.

Poniżej znajduje się przykład konfiguracji delegowania protokołu Kerberos (KCD) z następującymi założeniami:

- Punkt dostępu do protokołu mobilnego na Serwerze administracyjnym jest ustawiony na porcie 13292.
- Nazwa urządzenia z TMG to tmg.mydom.local.
- Nazwa urządzenia z Serwerem administracyjnym to ksc.mydom.local.
- Nazwa zewnętrznej publikacji punktu dostępu do protokołu mobilnego to kes4mob.mydom.global.

Konto domeny dla Serwera administracyjnego

Należy utworzyć konto domeny (na przykład: KSCMobileSrvcUsr), z poziomu którego będzie uruchamiana usługa Serwera administracyjnego. Konto dla usługi Serwera administracyjnego można określić podczas instalacji Serwera administracyjnego lub poprzez narzędzie klsrvswch. Narzędzie klsrvswch znajduje się w folderze instalacyjnym Serwera administracyjnego.

Konto domeny musi zostać określone z następujących względów:

- Funkcja zarządzania urządzeniami KES jest integralną częścią Serwera administracyjnego.
- Aby zapewnić poprawne działanie delegowania protokołu Kerberos (KCD), strona odbierająca (czyli Serwer administracyjny) musi być uruchomiona z poziomu konta domeny.

Nazwa główna usługi dla http/kes4mob.mydom.local

W domenie, z poziomu konta KSCMobileSrvcUsr, dodaj SPN dla publikacji usługi protokołu mobilnego na porcie 13292 urządzenia z Serwerem administracyjnym. Dla urządzenia kes4mob.mydom.local z Serwerem administracyjnym będzie to wyglądało w następujący sposób:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Konfigurowanie właściwości domeny urządzenia z TMG (tmg.mydom.local)

Aby przeprowadzić ruch sieciowy, przełącz urządzenie z TMG (tmg.mydom.local) do usługi, która jest definiowana po SPN (http/kes4mob.mydom.local:13292).

W celu przełączenia urządzenia z TMG do usługi definiowanej po SPN (http/kes4mob.mydom.local:13292), administrator musi wykonać następujące działania:

1. W przystawce Microsoft Management Console o nazwie „Użytkownicy i komputery usługi Active Directory" wybierz urządzenie z zainstalowanym TMG (tmg.mydom.local).

2. We właściwościach urządzenia, na zakładce **Delegowanie** ustaw przełącznik **Ufaj temu komputerowi w delegowaniu tylko do określonych usług** na **Użyj dowolnego protokołu uwierzytelniania**.

3. Na liście **Usługi, którym to konto może przedstawiać delegowane poświadczenia** dodaj SPN http/kes4mob.mydom.local:13292.

Specjalny (niestandardowy) certyfikat dla publikacji (kes4mob.mydom.global)

Aby opublikować protokół mobilny Serwera administracyjnego, należy wystawić specjalny (niestandardowy) certyfikat dla FQDN kes4mob.mydom.global, a także określić go w miejsce domyślnego certyfikatu serwera w ustawieniach protokołu mobilnego Serwera administracyjnego, w Konsoli administracyjnej. W tym celu, w oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat**.

Należy pamiętać, że kontener certyfikatów serwera (plik z rozszerzeniem .p12 lub .pfx) musi także zawierać łańcuch certyfikatów głównych (klucze publiczne).

Konfigurowanie publikacji na TMG

Na TMG, dla ruchu przechodzącego z urządzenia mobilnego do portu 13292 usługi kes4mob.mydom.global należy skonfigurować KCD na SPN (http/kes4mob.mydom.local:13292), korzystając z certyfikatu serwera opublikowanego dla FQDN kes4mob.mydom.global. Nie można zapominać, że publikacja oraz opublikowany punkt dostępu (port 13292 Serwera administracyjnego) powinny korzystać z tego samego certyfikatu serwera.

Korzystanie z Google Firebase Cloud Messaging

Aby zapewnić reakcję urządzeń KES z systemem Android w odpowiednim momencie na polecenia administratora, należy włączyć korzystanie z usługi Google™ Firebase Cloud Messaging (zwana również FCM) we właściwościach Serwera administracyjnego.

W celu włączenia korzystania z FCM:

1. W Konsoli administracyjnej wybierz węzeł **Zarządzanie urządzeniami mobilnymi** oraz folder **Urządzenia mobilne**.
2. Z otwartego menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.
3. We właściwościach folderu wybierz sekcję **Ustawienia Google Firebase Cloud Messaging**.
4. W polach **ID nadawcy** i **Klucz serwera** określ ustawienia FCM: ID_NADAWCY i Klucz API.

Usługa FCM działa w następujących zakresach adresów:

- Ze strony urządzenia KES dostęp jest wymagany do portów 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) oraz 5230 (HTTPS) dla następujących adresów:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169
- Ze strony Serwera administracyjnego dostęp jest wymagany do portu 443 (HTTPS) dla następujących adresów:
  - fcm.googleapis.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169

Jeśli ustawienia serwera proxy (**Zaawansowane** / **Konfiguracja dostępu do internetu**) zostały określone we właściwościach Serwera administracyjnego w Konsoli administracyjnej, będą używane do interakcji z FCM.

Konfigurowanie FCM: uzyskiwanie ID_NADAWCY i klucza API

W celu skonfigurowania FCM, administrator musi wykonać następujące akcje:

1. Zarejestrować się na portalu Google.
2. Przejść na portal deweloperów.
3. Utworzyć nowy projekt, klikając przycisk **Create Project**, określić nazwę projektu oraz ID.
4. Zaczekać, aż projekt zostanie utworzony.

   Na pierwszej stronie projektu, w górnej części strony pole **Project Number** wyświetli odpowiedni ID_NADAWCY.
5. Przejść do sekcji **APIs & auth / APIs** i włączyć **Google Firebase Cloud Messaging for Android**.
6. Przejść do sekcji **APIs & auth / Credentials** i kliknąć przycisk **Create New Key**.
7. Kliknij przycisk **Klucz serwera**.
8. Nałożyć ograniczenia (jeśli są) i kliknąć przycisk **Create**.
9. Uzyskać klucz API z właściwości nowo utworzonego klucza (pole **Klucz serwera**).

Integracja z infrastrukturą kluczy publicznych

Integracja z infrastrukturą kluczy publicznych (zwana również PKI) jest przeznaczona głównie do uproszenia wystawiania certyfikatów użytkownika domeny przez Serwer administracyjny.

Administrator może przypisać certyfikat domeny dla użytkownika w Konsoli administracyjnej. Można to zrobić przy użyciu jednej z następujących metod:

- Przydziel użytkownikowi specjalny (niestandardowy) certyfikat z pliku w kreatorze instalacji certyfikatu.
- Przeprowadź integrację z PKI i wskaż PKI jako źródło certyfikatów dla określonego typu certyfikatów lub dla wszystkich typów certyfikatów.

Ustawienia integracji z PKI są dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** po kliknięciu odnośnika **Zintegruj z infrastrukturą klucza publicznego**.

Ogólne zasady integracji z PKI dla publikacji certyfikatów użytkownika domeny

W Konsoli administracyjnej, w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** kliknij odnośnik **Zintegruj z infrastrukturą klucza publicznego**, aby określić konto domeny, które będzie używane przez Serwer administracyjny do wystawiania certyfikatów użytkownika domeny poprzez urząd certyfikacji domeny (zwany również kontem, z poziomu którego wykonywana jest integracja z PKI).

Należy pamiętać, że:

- Ustawienia integracji z PKI oferują możliwość określenia domyślnego szablonu dla wszystkich typów certyfikatów. Nie wolno też zapominać, że reguły wydawania certyfikatów (dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** po kliknięciu przycisku **Konfiguruj reguły wydawania certyfikatów**) pozwalają na określenie indywidualnego szablonu dla każdego typu certyfikatu.

- Specjalny certyfikat Agenta rejestracji (EA) powinien zostać zainstalowany na urządzeniu z Serwerem administracyjnym, w repozytorium certyfikatów konta, z poziomu którego wykonywana jest integracja z PKI. Certyfikat Agenta rejestracji (EA) jest wystawiany przez administratora urzędu certyfikacji domeny (CA).

Konto, z poziomu którego wykonywana jest integracja z PKI, musi spełniać następujące kryteria.

- Jest to użytkownik domeny.

- Jest to lokalny administrator urządzenia z Serwerem administracyjnym, z poziomu którego została zainicjowana integracja z PKI.

- Posiada uprawnienie do *Zalogowania w trybie usługi*.

- Urządzenie z zainstalowanym Serwerem administracyjnym musiało być wcześniej uruchomione przynajmniej raz z poziomu tego konta w celu utworzenia trwałego profilu użytkownika.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (zwany również serwerem sieciowym) jest składnikiem Kaspersky Security Center. Serwer sieciowy został zaprojektowany do publikowania autonomicznych pakietów instalacyjnych, autonomicznych pakietów instalacyjnych dla urządzeń mobilnych, profili iOS MDM oraz plików z folderu współdzielonego.

Profile iOS MDM oraz utworzone pakiety instalacyjne są automatycznie publikowane na serwerze sieciowym, a następnie są usuwane po pierwszym pobraniu. Administrator może wysłać użytkownikowi nowy odnośnik w dowolny sposób, na przykład za pośrednictwem poczty elektronicznej.

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

Ustawienia serwera sieciowego

Jeśli wymagane jest dostrojenie serwera sieciowego, właściwości serwera sieciowego w Konsoli administracyjnej oferują możliwość zmiany portów dla HTTP (8060) i HTTPS (8061). Oprócz zmiany portów, możesz zastąpić certyfikat serwera dla HTTPS i zmienić FQDN serwera sieciowego dla HTTP.

Instalacja Kaspersky Security Center

Ta sekcja opisuje instalację modułów programu Kaspersky Security Center. Jeśli chcesz zainstalować aplikację lokalnie tylko na jednym urządzeniu, dostępne są dwie opcje instalacji:

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

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

Jeśli w sieci jest zainstalowany przynajmniej jeden Serwer administracyjny, Serwery mogą być zdalnie instalowane na innych urządzeniach poprzez zadanie zdalnej instalacji przy użyciu instalacji wymuszonej. Podczas tworzenia zadania zdalnej instalacji należy użyć pakietu instalacyjnego Serwera administracyjnego: ksc_<version_number>.<build number>_full_<localization language>.exe.

Użyj tego pakietu, jeśli chcesz zainstalować wszystkie komponenty niezbędne do zapewnienia pełnej funkcjonalności Kaspersky Security Center lub do zaktualizowania bieżących wersji tych komponentów.

Jeśli chcesz wdrożyć klaster trybu failover Kaspersky, musisz zainstalować Kaspersky Security Center na wszystkich węzłach klastra.

Przygotowanie do instalacji

Przed rozpoczęciem instalacji postępuj zgodnie z instrukcjami podanymi w tym temacie.

- **Sprawdź wymagania sprzętowe i programowe**

  Upewnij się, że sprzęt i oprogramowanie urządzenia spełniają wymagania dla Serwera administracyjnego i Konsoli administracyjnej.

- **Wybierz i zainstaluj system zarządzania bazą danych (DBMS)**

  Kaspersky Security Center przechowuje swoje informacje w bazie danych zarządzanej przez DBMS. Zainstaluj DBMS w sieci przed Kaspersky Security Center (dowiedz się więcej o tym, jak wybrać DBMS). Jeśli zdecydujesz się zainstalować PostgreSQL lub Postgres Pro DBMS, podaj hasło dla superużytkownika. Jeśli hasło nie zostanie określone, Serwer administracyjny może nie być w stanie połączyć się z bazą danych.

  Zaleca się zainstalowanie Serwera administracyjnego na serwerze dedykowanym zamiast na kontrolerze domeny. Jeśli instalujesz Kaspersky Security Center na serwerze, który działa jako kontroler domeny tylko do odczytu (RODC), Microsoft SQL Server (SQL Express) nie może zostać zainstalowany lokalnie (na tym samym urządzeniu). W tym przypadku zalecane jest zdalne zainstalowanie Microsoft SQL Server (SQL Express) (na innym urządzeniu) lub tego, którego używasz — MySQL, MariaDB, lub PostgreSQL — jeśli musisz zainstalować system DBMS lokalnie.

  Zainstaluj Serwer administracyjny, Agenta sieciowego i Konsolę administracyjną w folderach, dla których uwzględnianie wielkości liter jest wyłączone. Dodatkowo, uwzględnianie wielkości liter musi być wyłączone dla folderu współdzielonego Serwera administracyjnego oraz ukrytego folderu Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

  Wersja serwerowa Agenta sieciowego zostanie zainstalowana na urządzeniu wraz z Serwerem administracyjnym. Serwer administracyjny nie może być zainstalowany wraz ze zwykłą wersją Agenta sieciowego. Jeśli serwerowa wersja Agenta sieciowego jest już zainstalowana na Twoim urządzeniu, usuń ją i ponownie uruchom instalację Serwera administracyjnego. Aby uzyskać szczegółowe informacje na temat wersji serwerowej Agenta sieciowego, zobacz Zmiany w systemie po instalacji Kaspersky Security Center.

- **Sprawdź konta**

  Instalacja Kaspersky Security Center wymaga uprawnień administratora na urządzeniu, na którym ma być ona przeprowadzona.

  Kaspersky Security Center obsługuje zarządzane konta usługi i grupę zarządzanych kont usługi. Jeśli te typy kont są używane w Twojej domenie i chcesz określić jedno z nich jako konto dla usługi serwera administracyjnego, najpierw zainstaluj to konto na tym samym urządzeniu, na którym chcesz zainstalować serwer administracyjny. Szczegółowe informacje na temat instalacji zarządzanych kont usług na urządzeniu lokalnym można znaleźć w oficjalnej dokumentacji firmy Microsoft.

Konta do pracy z DBMS

Aby zainstalować Serwer administracyjny i pracować z nim, potrzebujesz konta Windows, z poziomu którego uruchomisz instalator Serwera administracyjnego (zwanego dalej także instalatorem), konta Windows, z poziomu którego uruchomisz usługę Serwera administracyjnego oraz konto wewnętrzne DBMS, aby uzyskać dostęp do DBMS. Możesz tworzyć nowe konta lub korzystać z istniejących. Wszystkie te konta wymagają określonych uprawnień. Zestaw wymaganych kont i ich uprawnień zależy od następujących kryteriów:

- Typ DBMS:
  - Microsoft SQL Server (z uwierzytelnieniem Windows lub uwierzytelnieniem SQL Server)
  - MySQL lub MariaDB
  - PostgreSQL lub Postgres Pro
- Lokalizacja DBMS:
  - **Lokalny DBMS**. *Lokalny system DBMS* to system DBMS zainstalowany na tym samym urządzeniu co Serwer administracyjny.
  - **Zdalny DBMS**. *Zdalny system DBMS* to system DBMS zainstalowany na innym urządzeniu.
- Metoda tworzenia bazy danych Serwera administracyjnego:
  - **Automatyczne**. Podczas instalacji Serwera administracyjnego możesz automatycznie utworzyć bazę danych Serwera administracyjnego (zwaną dalej także bazą danych Serwera) przy użyciu instalatora.
  - **Ręcznie**. Możesz użyć aplikacji innej firmy (na przykład SQL Server Management Studio) lub skryptu, aby utworzyć pustą bazę danych. Następnie możesz określić tę bazę danych jako bazę danych Serwera podczas instalacji Serwera administracyjnego.

Przestrzegaj zasady najmniejszych uprawnień, gdy przyznajesz prawa i uprawnienia do kont. Oznacza to, że przyznane uprawnienia powinny wystarczyć tylko do wykonania wymaganych działań.

Poniższe tabele zawierają informacje o uprawnieniach systemowych i DBMS, które należy nadać kontom przed zainstalowaniem i uruchomieniem Serwera administracyjnego.

Microsoft SQL Server z uwierzytelnianiem Windows

Jeśli wybierzesz SQL Server jako DBMS, możesz użyć uwierzytelniania Windows, aby uzyskać dostęp do SQL Server. Skonfiguruj uprawnienia systemowe konta Windows używanego do uruchamiania instalatora oraz konta Windows używanego do uruchamiania usługi Serwera administracyjnego. W SQL Server utwórz loginy do obu tych kont Windows. W zależności od metody tworzenia bazy danych Serwera, nadaj tym kontom wymagane uprawnienia SQL Server, jak opisano w poniższej tabeli. Aby uzyskać więcej informacji na temat konfigurowania uprawnień kont, zobacz Konfigurowanie kont do pracy z SQL Server (uwierzytelnianie Windows).

DBMS: Microsoft SQL Server (w tym Express Edition) z uwierzytelnianiem systemu Windows

	Automatyczne tworzenie bazy danych (przez instalator)	Ręczne tworzenie bazy danych (przez Administratora)
Konto, z poziomu którego uruchomiony jest instalator	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia,	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest

	na którym zainstalowany jest DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.	DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.

Uprawnienia konta, z poziomu którego uruchomiony jest instalator	• Uprawnienia systemowe: uprawnienia lokalnego administratora.
	• Uprawnienia SQL Server:
	  • Rola na poziomie serwera: sysadmin.
		• Uprawnienia systemowe: uprawnienia lokalnego administratora.
		• Uprawnienia SQL Server:
		  • Rola na poziomie serwera: publiczna.
		  • Rola członka bazy danych w bazie danych serwera: db_owner, publiczna.
		  • Domyślny schemat bazy danych serwera: dbo.

Konto usługi Serwera administracyjnego	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS.
	• Lokalny DBMS:
	  • Konto Windows wybrane przez administratora.
	  • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.
		• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS.
		• Lokalny DBMS:
		  • Konto Windows wybrane przez administratora.
		  • Konto w formacie KL-AK-*, które instalator tworzy automatycznie (w tym przypadku nie zalecamy generowania konta KL-AK-*).

Uprawnienia dla konta usługi Serwera administracyjnego	• Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.
	• Uprawnienia SQL Server: wymagane uprawnienia, przypisane przez instalator.
		• Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.
		• Uprawnienia SQL Server:
		  • Rola na poziomie serwera: publiczna.
		  • Rola członka bazy danych w bazie danych serwera: db_owner, publiczna.
		  • Domyślny schemat bazy danych serwera: dbo.

Microsoft SQL Server z uwierzytelnieniem SQL Server

Jeśli wybierzesz SQL Server jako DBMS, możesz użyć uwierzytelniania Serwery SQL, aby uzyskać dostęp do SQL Server. Skonfiguruj uprawnienia systemowe konta Windows używanego do uruchamiania instalatora oraz konta Windows używanego do uruchamiania usługi Serwera administracyjnego. W SQL Server utwórz login z hasłem, aby użyć go do uwierzytelnienia. Następnie nadaj temu kontu SQL Server wymagane uprawnienia wymienione w poniższej tabeli. Aby uzyskać więcej informacji na temat konfigurowania uprawnień kont, zobacz Konfigurowanie kont do pracy z SQL Server (uwierzytelnienie SQL Server).

DBMS: Microsoft SQL Server (w tym Express Edition) z uwierzytelnianiem SQL Server

	Automatyczne tworzenie bazy danych (przez instalator)	**Ręczne tworzenie bazy danych (przez Administratora)**
Konto, z poziomu którego uruchomiony jest instalator	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.
Uprawnienia konta, z poziomu którego uruchomiony jest instalator	Uprawnienia systemowe: uprawnienia lokalnego administratora.	Uprawnienia systemowe: uprawnienia lokalnego administratora.

Konto usługi Serwera administracyjnego	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS.
	• Lokalny DBMS:
	  • Konto Windows wybrane przez administratora.
	  • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.
		• Zdalny DBMS: tylko konto domeny zdalnego urządzenia, na którym zainstalowany jest DBMS.
		• Lokalny DBMS:
		  • Konto użytkownika Windows wybrane przez administratora.
		  • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.

Uprawnienia dla konta usługi Serwera administracyjnego	Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.	Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.

Prawa logowania używane do uwierzytelniania SQL Server	Uprawnienia SQL Server wymagane do utworzenia bazy danych i zainstalowania Serwera administracyjnego:
	• Rola na poziomie serwera: publiczna.
	• Rola członka bazy danych w *głównej* bazie danych: db_owner.
	• Domyślny schemat *głównej* bazy danych: dbo.
	• Uprawnienia:
	  • PODŁĄCZ DOWOLNĄ BAZĘ DANYCH
		Uprawnienia SQL Server:
		• Rola na poziomie serwera: publiczna.
		• Rola członka bazy danych w bazie danych serwera: db_owner.
		• Domyślny schemat bazy danych serwera: dbo.
		• Uprawnienia:
		  • PODŁĄCZ SQL
		  • PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH

	• PODŁĄCZ SQL • UTWÓRZ DOWOLNĄ BAZĘ DANYCH • PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH Uprawnienia SQL Server wymagane do pracy z Serwerem administracyjnym: • Rola na poziomie serwera: publiczna. • Rola członka bazy danych w bazie danych serwera: db_owner. • Domyślny schemat bazy danych serwera: dbo. • Uprawnienia: • PODŁĄCZ SQL • PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH	

Konfigurowanie uprawnień SQL Server do odzyskiwania danych Serwera administracyjnego

Aby przywrócić dane Serwera administracyjnego z kopii zapasowej, uruchom narzędzie klbackup z poziomu konta Windows użytego do zainstalowania Serwera administracyjnego. Przed uruchomieniem narzędzia klbackup na serwerze SQL Server nadaj uprawnienia do logowania do serwera SQL skojarzonego z tym kontem systemu Windows. Uprawnienia SQL Server różnią się w zależności od wersji Serwera administracyjnego. W przypadku Serwera administracyjnego w wersji 14.2 lub nowszej możesz nadać rolę na poziomie serwera sysadmin lub rolę na poziomie serwera dbcreator.

Uprawnienia SQL Server do odzyskiwania bazy danych Serwera administracyjnego

Serwer administracyjny w wersji 14.2 lub nowszej	**Inne wersje Serwera administracyjnego**
• Uprawnienia SQL Server: • Rola na poziomie serwera: sysadmin.	• Uprawnienia SQL Server: • Rola na poziomie serwera: sysadmin.
• Uprawnienia SQL Server: • Rola na poziomie serwera: dbcreator. • Uprawnienia: • WYŚWIETL DOWOLNĄ DEFINICJĘ	

Przed uruchomieniem narzędzia klbackup określ flagę serwera KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. Aby to zrobić, wykonaj następujące polecenie w wierszu poleceń:

```
klscflag.exe -fset -pv klserver -n
KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1
```

MySQL i MariaDB

Jeśli wybierzesz MySQL lub MariaDB jako DBMS, utwórz wewnętrzne konto DBMS i nadaj temu kontu wymagane uprawnienia wymienione w poniższej tabeli. Instalator i usługa Serwera administracyjnego używają tego wewnętrznego konta DBMS do uzyskiwania dostępu do DBMS. Należy pamiętać, że sposób tworzenia bazy danych nie wpływa na zestaw wymaganych uprawnień. Aby uzyskać więcej informacji na temat konfigurowania uprawnień konta, zobacz Konfigurowanie kont do pracy z MySQL i MariaDB.

DBMS: MySQL i MariaDB

	Automatyczne lub ręczne tworzenie bazy danych
Konto, z poziomu którego uruchomiony jest instalator	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.
Uprawnienia konta, z poziomu którego uruchomiony jest instalator	Uprawnienia systemowe: uprawnienia lokalnego administratora.

Konto usługi Serwera administracyjnego	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS.
	• Lokalny DBMS:
	  • Konto Windows wybrane przez administratora.
	  • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.

Uprawnienia dla konta usługi Serwera administracyjnego	Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.
Uprawnienia konta wewnętrznego DBMS	Uprawnienia dotyczące schematu: • Baza danych Serwera administracyjnego: ALL (oprócz GRANT OPTION). • Schematy systemowe (mysql i sys): SELECT, SHOW VIEW. • Procedura składowana sys.table_exists: EXECUTE (jeśli używasz MariaDB 10.5 lub wcześniejszej jako DBMS, nie musisz nadawać uprawnienia EXECUTE). Globalne uprawnienia dla wszystkich schematów: PROCESS, SUPER.

Konfigurowanie uprawnień do odzyskiwania danych Serwera administracyjnego

Uprawnienia nadane wewnętrznemu kontu DBMS wystarczą do przywrócenia danych Serwera administracyjnego z kopii zapasowej. Aby rozpocząć przywracanie, uruchom narzędzie klbackup z poziomu konta Windows użytego do zainstalowania Serwera administracyjnego.

PostgreSQL lub Postgres Pro

Jeśli wybierzesz PostgreSQL lub Postgres Pro jako DBMS, możesz użyć użytkownika *postgres* (domyślna rola Postgres) lub utworzyć nową rolę Postgres (zwaną dalej także rolą), aby uzyskać dostęp do DBMS. W zależności od metody tworzenia bazy danych Serwera, nadaj roli wymagane uprawnienia zgodnie z opisem w poniższej tabeli. Aby uzyskać więcej informacji na temat konfigurowania uprawnień roli, zobacz Konfigurowanie kont do pracy z PostgreSQL lub Postgres Pro.

DBMS: PostgreSQL lub Postgres Pro

	Automatyczne tworzenie bazy danych		Ręczne tworzenie bazy danych
Konto, z poziomu którego uruchomiony jest instalator	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.		• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS. • Lokalny DBMS: konto administratora lokalnego lub konto domeny.
Uprawnienia konta, z poziomu którego uruchomiony jest instalator	Uprawnienia systemowe: uprawnienia lokalnego administratora.		Uprawnienia systemowe: uprawnienia lokalnego administratora.

Konto usługi Serwera administracyjnego	• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS.
	• Lokalny DBMS:
	  • Konto Windows wybrane przez administratora.
	  • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.
			• Zdalny DBMS: tylko konto domeny zdalnego urządzenia z zainstalowanym DBMS.
			• Lokalny DBMS:
			  • Konto Windows wybrane przez administratora.
			  • Konto w formacie KL-AK-*, które instalator tworzy automatycznie.

Uprawnienia dla konta usługi Serwera administracyjnego	Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.		Uprawnienia systemowe: wymagane uprawnienia, przypisane przez instalator.
Uprawnienia roli Postgres	Użytkownik *postgres* nie wymaga dodatkowych uprawnień.	Uprawnienia nowej roli: `CREATEDB`.	Do nowej roli: • Uprawnienia w bazie danych Serwera administracyjnego: `ALL`. • Uprawnienia do wszystkich tabel w schemacie publicznym: `ALL`.

			• Uprawnienia do wszystkich sekwencji w schemacie publicznym: `ALL`.

Konfigurowanie uprawnień do odzyskiwania danych Serwera administracyjnego

Aby przywrócić dane Serwera administracyjnego z kopii zapasowej, uruchom narzędzie klbackup z poziomu konta Windows użytego do zainstalowania Serwera administracyjnego. Należy pamiętać, że rola Postgres używana do uzyskiwania dostępu do DBMS musi mieć uprawnienia właściciela do bazy danych Serwera administracyjnego.

Konfigurowanie kont do pracy z SQL Server (uwierzytelnianie Windows)

Wymagania wstępne

Przed przypisaniem uprawnień do kont wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.
2. Zainstaluj środowisko do pracy z SQL Server.
3. Upewnij się, że posiadasz konto Windows, z poziomu którego zainstalujesz Serwer administracyjny.
4. Upewnij się, że posiadasz konto Windows, z poziomu którego uruchomisz Serwer administracyjny.
5. Na SQL Server utwórz login konta Windows używanego do uruchamiania instalatora Serwera administracyjnego (zwanego dalej instalatorem). Utwórz również login dla konta Windows używanego do uruchamiania usługi Serwera administracyjnego.

Jeśli korzystasz z SQL Server Management Studio, na stronie **Ogólne** okna właściwości logowania wybierz opcję **Uwierzytelnianie systemu Windows**.

Konfigurowanie kont do instalacji Serwera administracyjnego (automatyczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. W SQL Server przypisz rolę sysadmin na poziomie serwera do loginu konta Windows używanego do uruchomienia instalatora.
2. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.
3. Uruchom instalator Serwera administracyjnego.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.
4. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.
5. Wybierz Microsoft SQL Server jako system DBMS przechowujący bazę danych Serwera administracyjnego.

6. Wybierz tryb Uwierzytelniania systemu Microsoft Windows, aby nawiązać połączenie między Serwerem administracyjnym a serwerem SQL za pośrednictwem konta Windows.

7. Określ nazwę konta Windows , aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać konto użytkownika systemu Windows, dla którego wcześniej utworzono login SQL Server. Alternatywnie możesz automatycznie utworzyć nowe konto Windows w formacie KL-AK-* za pomocą instalatora. W takim przypadku instalator automatycznie utworzy login SQL Server do tego konta. Niezależnie od wyboru konta, instalator przypisuje wymagane uprawnienia systemowe oraz uprawnienia SQL Server do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji tworzona jest baza danych Serwera, a wszystkie wymagane uprawnienia systemowe i uprawnienia SQL Server są przypisywane do konta usługi Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Konfigurowanie kont do instalacji Serwera administracyjnego (ręczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Na SQL Server utwórz pustą bazę danych. Ta baza danych będzie używana jako baza danych Serwera administracyjnego (zwana dalej również bazą danych Serwera).

2. Dla obu loginów SQL Server utworzonych dla kont Windows określ rolę na poziomie serwera publicznego, a następnie skonfiguruj mapowanie do utworzonej bazy danych:

   - Rola na poziomie serwera: publiczna
   - Przynależność do roli bazy danych: db_owner, public
   - Domyślny schemat: dbo

3. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.

4. Uruchom instalator Serwera administracyjnego.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

5. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.

6. Wybierz Microsoft SQL Server jako system DBMS przechowujący bazę danych Serwera administracyjnego.

7. Określ nazwę utworzonej bazy danych jako nazwę bazy danych Serwera administracyjnego.

8. Wybierz tryb Uwierzytelniania systemu Microsoft Windows, aby nawiązać połączenie między Serwerem administracyjnym a serwerem SQL za pośrednictwem konta Windows.

9. Określ nazwę konta Windows , aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać konto użytkownika Windows, dla którego utworzono login SQL Server i wcześniej skonfigurowano prawa logowania.

Nie zalecamy automatycznego tworzenia nowego konta Windows w formacie KL-AK-*. W takim przypadku instalator tworzy nowe konto Windows, do którego nie utworzono i nie skonfigurowano konta SQL Server. Serwer administracyjny nie może użyć tego konta do uruchomienia usługi Serwera administracyjnego. Jeżeli konieczne jest utworzenie konta KL-AK-* Windows, nie uruchamiaj Konsoli administracyjnej po zakończeniu instalacji. Zamiast tego wykonaj następujące czynności:

1. Zatrzymaj usługę kladminserver.
2. Na SQL Server utwórz login SQL Server do utworzonego konta KL-AK-* Windows.
3. Przyznaj prawa do tego loginu SQL Server i skonfiguruj mapowanie do utworzonej bazy danych:
   - Rola na poziomie serwera: publiczna
   - Przynależność do roli bazy danych: db_owner, public
   - Domyślny schemat: dbo
4. Zrestartuj usługę kladminserver, a następnie uruchom Konsolę administracyjną.

Po zakończeniu instalacji Serwer administracyjny użyje utworzonej bazy danych do przechowywania danych Serwera. Serwer administracyjny jest gotowy do użycia.

Konfigurowanie kont do pracy z SQL Server (uwierzytelnianie SQL Server)

Wymagania wstępne

Przed przypisaniem uprawnień do kont wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.
2. Zainstaluj środowisko do pracy z SQL Server.
3. Upewnij się, że posiadasz konto Windows, z poziomu którego zainstalujesz Serwer administracyjny.
4. Upewnij się, że posiadasz konto Windows, z poziomu którego uruchomisz Serwer administracyjny.
5. W SQL Server włącz tryb uwierzytelniania SQL Server.

   Jeśli korzystasz z programu SQL Server Management Studio, w oknie Właściwości programu SQL Server na stronie **Zabezpieczenia** wybierz opcję **Tryb uwierzytelniania programu SQL Server i systemu Windows**.
6. W SQL Server utwórz login z hasłem. Instalator Serwera administracyjnego (zwany dalej także instalatorem) oraz usługa Serwera administracyjnego będą używać tego konta SQL Server do uzyskiwania dostępu do SQL Server.

   Jeśli korzystasz z SQL Server Management Studio, na stronie **Ogólne** okna właściwości logowania wybierz opcję **Uwierzytelnianie SQL Server.**

Konfigurowanie kont do instalacji Serwera administracyjnego (automatyczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. W SQL Server zamapuj konto SQL Server na domyślną *główną* bazę danych. *Główna* baza danych będzie używana jako baza danych Serwera administracyjnego (zwana dalej również bazą danych Serwera). Główna *baza* danych jest używana do mapowania, dopóki instalator nie utworzy bazy danych Serwera. Przyznaj następujące prawa i uprawnienia do konta SQL Server:
   - Rola na poziomie serwera: publiczna

- Rola członka bazy danych w *głównej* bazie danych: db_owner
- Domyślny schemat *głównej* bazy danych: dbo
- Uprawnienia:
  - PODŁĄCZ DOWOLNĄ BAZĘ DANYCH
  - PODŁĄCZ SQL
  - UTWÓRZ DOWOLNĄ BAZĘ DANYCH
  - PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH

2. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.
3. Uruchom instalator.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.
4. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.
5. Wybierz Microsoft SQL Server jako system DBMS przechowujący bazę danych Serwera administracyjnego.
6. Określ Nazwa bazy danych Serwera administracyjnego.
7. Wybierz tryb Uwierzytelniania SQL Server, aby nawiązać połączenie między Serwerem administracyjnym a SQL Server za pośrednictwem utworzonego konta SQL Server. Następnie określ poświadczenia konta SQL Server.
8. Określ nazwę konta Windows , aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać istniejące konto użytkownika Windows lub utworzyć nowe konto Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji tworzona jest baza danych Serwera i wszystkie wymagane uprawnienia systemowe są przypisywane do konta usługi Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Możesz anulować mapowanie do *głównej* bazy danych, ponieważ instalator utworzył bazę danych Serwera i skonfigurował mapowanie do tej bazy danych podczas instalacji Serwera administracyjnego.

Ponieważ automatyczne tworzenie bazy danych wymaga większych uprawnień niż normalna praca z Serwerem administracyjnym, możesz cofnąć niektóre uprawnienia. Na SQL Server wybierz konto SQL Server, a następnie nadaj następujące uprawnienia do pracy z Serwerem administracyjnym:

- Rola na poziomie serwera: publiczna
- Rola członka bazy danych w bazie danych serwera: db_owner
- Domyślny schemat bazy danych serwera: dbo
- Uprawnienia:
  - PODŁĄCZ SQL
  - PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH

Konfigurowanie kont do instalacji Serwera administracyjnego (ręczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Na SQL Server utwórz pustą bazę danych. Ta baza danych będzie używana jako baza danych Serwera administracyjnego.
2. W SQL Server przyznaj następujące prawa i uprawnienia do konta SQL Server:
   - Rola na poziomie serwera: publiczna.
   - Rola członka bazy danych w utworzonej bazie danych: db_owner.
   - Domyślny schemat utworzonej bazy danych: dbo.
   - Uprawnienia:
     - PODŁĄCZ SQL
     - PRZEGLĄDAJ DOWOLNĄ BAZĘ DANYCH
3. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.
4. Uruchom instalator.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.
5. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.
6. Wybierz Microsoft SQL Server jako system DBMS przechowujący bazę danych Serwera administracyjnego.
7. Określ nazwę utworzonej bazy danych jako nazwę bazy danych Serwera administracyjnego.
8. Wybierz tryb Uwierzytelniania SQL Server, aby nawiązać połączenie między Serwerem administracyjnym a SQL Server za pośrednictwem utworzonego konta SQL Server. Następnie określ poświadczenia konta SQL Server.
9. Określ nazwę konta Windows , aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać istniejące konto użytkownika Windows lub utworzyć nowe konto Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji Serwer administracyjny użyje utworzonej bazy danych do przechowywania danych Serwera administracyjnego. Wszystkie wymagane uprawnienia systemowe są przypisane do konta usługi Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Konfiguracja kont do pracy z MySQL i MariaDB

Wymagania wstępne

Przed przypisaniem uprawnień do kont wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.

2. Zainstaluj środowisko do pracy z MySQL lub MariaDB.
3. Upewnij się, że posiadasz konto Windows, z poziomu którego zainstalujesz Serwer administracyjny.
4. Upewnij się, że posiadasz konto Windows, z poziomu którego uruchomisz Serwer administracyjny.

Konfigurowanie kont do instalacji Serwera administracyjnego

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z MySQL lub MariaDB na koncie root, które utworzono podczas instalacji DBMS.
2. Utwórz wewnętrzne konto DBMS z hasłem. Instalator Serwera administracyjnego (zwany dalej także instalatorem) oraz usługa Serwera administracyjnego będą używać tego wewnętrznego konta DBMS do uzyskiwania dostępu do DBMS. Nadaj temu kontu następujące uprawnienia:
   - Uprawnienia dotyczące schematu:
     - Baza danych Serwera administracyjnego: WSZYSTKIE (oprócz `GRANT OPTION`)
     - Schematy systemowe (mysql i sys): `SELECT`, `SHOW VIEW`
     - Procedura składowana sys.table_exists: `EXECUTE`
   - Globalne uprawnienia dla wszystkich schematów: `PROCESS`, `SUPER`

   Aby utworzyć wewnętrzne konto DBMS i nadać mu wymagane uprawnienia, uruchom poniższy skrypt (w tym skrypcie login DBMS to *KCSAdmin*, nazwa bazy danych Serwera administracyjnego to *kav*):

```
/* Utwórz użytkownika o nazwie KSCAdmin */
CREATE USER 'KSCAdmin'
/* Określ hasło KSCAdmin */
IDENTIFIED BY '<password>';
/* Przyznaj uprawnienia KSCAdmin */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

   > Jeśli używasz MariaDB 10.5 lub wersji starszej jako DBMS, nie musisz nadawać uprawnienia EXECUTE. W takim przypadku wyklucz następujące polecenie ze skryptu: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

3. Aby wyświetlić listę uprawnień nadanych kontu DBMS, uruchom następujący skrypt:

```
SHOW grants for 'KSCAdmin'
```

4. Aby utworzyć bazę danych Serwera administracyjnego, uruchom następujący skrypt (w tym skrypcie nazwa bazy danych Serwera administracyjnego to *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET 'ascii'
   COLLATE 'ascii_general_ci';
   ```

   Użyj tej samej nazwy bazy danych co określona w skrypcie tworzącym konto DBMS.

5. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.

6. Uruchom instalator.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

7. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.

8. Wybierz MySQL lub MariaDB jako system DBMS przechowujący bazę danych Serwera administracyjnego.

9. Określ Nazwa bazy danych Serwera administracyjnego. Użyj tej samej nazwy bazy danych co określona w skrypcie.

10. Określ poświadczenia konta DBMS utworzonego przez skrypt.

11. Określ nazwę konta Windows , aby uruchomić usługę Serwera administracyjnego.

    Możesz wybrać istniejące konto użytkownika systemu Windows lub automatycznie utworzyć nowe konto systemu Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji baza danych Serwera administracyjnego jest tworzona i Serwer administracyjny jest gotowy do użycia.

Konfiguracja kont do pracy z PostgreSQL i Postgres Pro

Wymagania wstępne

Przed przypisaniem uprawnień do kont wykonaj następujące czynności:

1. Upewnij się, że logujesz się do systemu na konto administratora lokalnego.

2. Zainstaluj środowisko do pracy z PostgreSQL i Postgres Pro.

3. Upewnij się, że posiadasz konto Windows, z poziomu którego zainstalujesz Serwer administracyjny.

4. Upewnij się, że posiadasz konto Windows, z poziomu którego uruchomisz Serwer administracyjny.

Konfigurowanie kont do instalacji Serwera administracyjnego (automatyczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z PostgreSQL i Postgres Pro.

2. Wybierz rolę Postgres, aby uzyskać dostęp do DBMS. Możesz wybrać jedną z następujących opcji:

   - Użytkownik *postgres* (domyślna rola Postgres).

     Jeśli używasz użytkownika *postgres*, nie musisz nadawać mu dodatkowych uprawnień.

   - Nowa rola Postgres.

     Jeśli chcesz użyć nowej roli Postgres, utwórz tę rolę, a następnie nadaj jej uprawnienie CREATEDB. W tym celu uruchom następujący skrypt (w tym skrypcie rolą jest *KCSAdmin*):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<password>' CREATEDB;
     ```

     Utworzona rola będzie używana jako właściciel bazy danych Serwera administracyjnego (zwanej dalej również Bazą danych Serwera).

3. Zaloguj się do systemu z poziomu konta Windows używanego do uruchomienia instalatora Serwera administracyjnego (zwanego dalej także instalatorem).

4. Uruchom instalator.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

5. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.

6. Wybierz PostgreSQL lub Postgres Pro jako system DBMS przechowujący bazę danych Serwera administracyjnego.

7. Określ Nazwa bazy danych Serwera. Instalator automatycznie utworzy bazę danych Serwera.

8. Określ poświadczenia roli Postgres.

9. Określ nazwę konta Windows , aby uruchomić usługę Serwera administracyjnego.

   Możesz wybrać istniejące konto użytkownika systemu Windows lub automatycznie utworzyć nowe konto systemu Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji baza danych Serwera jest tworzona automatycznie i Serwer administracyjny jest gotowy do użycia.

Konfigurowanie kont do instalacji Serwera administracyjnego (ręczne tworzenie bazy danych Serwera administracyjnego)

W celu skonfigurowania konta instalacji Serwera administracyjnego:

1. Uruchom środowisko do pracy z Postgres.

2. Utwórz nową rolę Postgres i bazę danych Serwera administracyjnego. Następnie nadaj roli wszystkie uprawnienia w bazie danych Serwera administracyjnego. W tym celu zaloguj się jako użytkownik *postgres* w bazie danych *postgres* i uruchom następujący skrypt (w tym skrypcie rola to *KCSAdmin*, nazwa bazy danych Serwera administracyjnego to *KAV*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<password>';
   CREATE DATABASE "KAV" ENCODING 'UTF8';
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

3. Nadaj następujące uprawnienia utworzonej roli Postgres:

- Uprawnienia do wszystkich tabel w schemacie publicznym: ALL
- Uprawnienia do wszystkich sekwencji w schemacie publicznym: ALL

W tym celu zaloguj się jako użytkownik *postgres* w bazie danych Serwera i uruchom następujący skrypt (w tym skrypcie rola to *KCSAdmin*):

```
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
```

4. Zaloguj się do systemu na konto Windows użyte do uruchomienia instalatora.
5. Uruchom instalator Serwera administracyjnego.

   Uruchomi się kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.
6. Wybierz opcję niestandardowej instalacji Serwera administracyjnego.
7. Wybierz PostgreSQL lub Postgres Pro jako system DBMS przechowujący bazę danych Serwera administracyjnego.
8. Określ Nazwa bazy danych Serwera. Użyj tej samej nazwy bazy danych co określona w skrypcie. Należy pamiętać, że w nazwie bazy danych rozróżniana jest wielkość liter.
9. Określ poświadczenia roli Postgres.
10. Określ nazwę konta Windows , aby uruchomić usługę Serwera administracyjnego.

    Możesz wybrać istniejące konto użytkownika systemu Windows lub automatycznie utworzyć nowe konto systemu Windows w formacie KL-AK-* za pomocą instalatora. Niezależnie od wyboru konta instalator przypisuje wymagane uprawnienia systemowe do konta usługi Serwera administracyjnego.

Po zakończeniu instalacji Serwer administracyjny użyje utworzonej bazy danych do przechowywania danych Serwera administracyjnego. Serwer administracyjny jest gotowy do użycia.

Scenariusz: Autoryzacja Microsoft SQL Server

Informacje w tej sekcji są stosowane tylko do konfiguracji, w których Kaspersky Security Center używa Microsoft SQL Server jako systemu zarządzania bazą danych.

Aby chronić dane Kaspersky Security Center przesyłane do lub z bazy danych oraz dane przechowywane w bazie danych przed nieautoryzowanym dostępem, musisz zabezpieczyć komunikację między Kaspersky Security Center a SQL Server. Najbardziej rozsądny sposób zapewnienia bezpiecznej komunikacji to zainstalowanie Kaspersky Security Center i SQL Server na tym samym urządzeniu i używanie mechanizmu pamięci współużytkowanej dla obu aplikacji. We wszystkich pozostałych przypadkach zalecane jest użycie certyfikatu SSL lub TLS do autoryzacji instancji SQL Server. Możesz użyć certyfikatu z zaufanego urzędu certyfikacji lub certyfikatu z podpisem własnym. Zalecane jest użycie certyfikatu z zaufanego urzędu certyfikacji, ponieważ certyfikat z podpisem własnym zapewnia tylko ograniczoną ochronę.

Autoryzacja SQL Server odbywa się w etapach:

1. **Generowanie certyfikatu SSL lub TLS z podpisem własnym dla SQL Server zgodnie z wymaganiami certyfikatu**

   Jeśli już posiadasz certyfikat dla SQL Server, pomiń ten krok.

Certyfikat SSL jest stosowany tylko do wersji SQL Server wcześniejszych niż 2016 (13.x). W SQL Server 2016 (13.x) i nowszych wersjach użyj certyfikatu TLS.

Na przykład, aby wygenerować certyfikat TLS, wprowadź następujące polecenie w PowerShell:

```
New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
-KeySpec KeyExchange
```

W poleceniu zamiast SQL_HOST_NAME należy wpisać nazwę hosta SQL Server, jeśli host znajduje się w domenie lub wpisz *w pełni kwalifikowaną nazwę domeny* (FQDN) hosta, jeśli host nie znajduje się w domenie. Taka sama nazwa — nazwa hosta lub FQDN — musi być określona jako nazwa instancji SQL Server w kreatorze instalacji Serwera administracyjnego.

2. **Dodawanie certyfikatu na instancji SQL Server**

   Instrukcje dla tego etapu zależą od platformy, na której uruchomiony jest SQL Server. Więcej informacji można znaleźć w oficjalnej dokumentacji:

   - Windows
   - Linux
   - Amazon Relational Database Service
   - Windows Azure

   Aby użyć certyfikatu na klastrze typu failover, należy zainstalować certyfikat na każdym węźle klastra typu failover. Więcej informacji znajdziesz w dokumentacji Microsoft.

3. **Przypisywanie uprawnień konta usługi**

   Upewnij się, że konto usługi, z poziomu którego usługa SQL Server jest uruchomiona, posiada uprawnienie dostępu Pełna kontrola do kluczy prywatnych. Więcej informacji znajdziesz w dokumentacji Microsoft.

4. **Dodawanie certyfikatu do listy zaufanych certyfikatów dla Kaspersky Security Center**

   Na urządzeniu Serwer administracyjny dodaj certyfikat do listy zaufanych certyfikatów. Więcej informacji znajdziesz w dokumentacji Microsoft.

5. **Włączanie połączeń szyfrowanych między instancją SQL Server a Kaspersky Security Center**

   Na urządzeniu Serwera administracyjnego ustaw wartość `1` dla zmiennej środowiskowej `KLDBADO_UseEncryption`. Na przykład, w systemie Windows Server 2012 R2 możesz zmienić zmienne środowiskowe, klikając **Zmienne środowiskowe** na zakładce **Zaawansowane** okna **Właściwości systemu**. Dodaj nową zmienną, nazwij ją `KLDBADO_UseEncryption`, a następnie ustaw wartość `1`.

6. **Dodatkowa konfiguracja do użycia protokołu TLS 1.2**

   Jeśli używasz protokołu TLS 1.2, wówczas dodatkowo wykonaj następujące czynności:

   - Upewnij się, że zainstalowana wersja SQL Server to 64-bitowa aplikacja.
   - Zainstaluj sterownik Microsoft OLE DB Driver na urządzeniu Serwera administracyjnego. Więcej informacji znajdziesz w dokumentacji Microsoft.
   - Na urządzeniu Serwera administracyjnego ustaw wartość `1` dla zmiennej środowiskowej `KLDBADO_UseMSOLEDBSQL`. Na przykład, w systemie Windows Server 2012 R2 możesz zmienić zmienne środowiskowe, klikając **Zmienne środowiskowe** na zakładce **Zaawansowane** okna **Właściwości systemu**. Dodaj nową zmienną, nazwij ją `KLDBADO_UseMSOLEDBSQL`, a następnie ustaw wartość `1`.

Jeśli wersja sterownika OLE DB to 19 lub nowsza, ustaw również wartość `MSOLEDBSQL19` na zmienną środowiskową `KLDBADO_ProviderName`.

7. **Włączanie użycia protokołu TCP/IP na nazwanej instancji SQL Server**

   Jeśli używasz nazwanej instancji SQL Server, dodatkowo włącz użycie protokołu TCP/IP i przypisz numer portu TCP/IP do aparatu bazy danych SQL Server. Jeśli skonfigurujesz połączenie SQL Server w kreatorze instalacji Serwera administracyjnego, określ numer portu oraz nazwę hosta SQL Server w polu **Nazwa instancji SQL Server**.

Zalecenia dotyczące instalacji Serwera administracyjnego

Ta sekcja zawiera zalecenia dotyczące instalacji Serwera administracyjnego. Opisane są tu także scenariusze korzystania z folderu współdzielonego na urządzeniu z Serwerem administracyjnym w celu zainstalowania Agenta sieciowego na urządzeniach klienckich.

Tworzenie kont dla usług Serwera administracyjnego na klastrze typu failover

Domyślnie instalator automatycznie tworzy konta bez uprawnień dla usług Serwera administracyjnego. To zachowanie jest najwygodniejsze w przypadku instalacji Serwera administracyjnego na zwykłym urządzeniu.

Jednakże instalacja Serwera administracyjnego na klastrze typu failover wymaga innego scenariusza:

1. Dla usług Serwera administracyjnego utwórz konta domenowe bez uprawnień i przydziel je do globalnej grupy zabezpieczeń w domenie o nazwie KLAdmins.

2. W instalatorze Serwera administracyjnego określ konta domenowe, które zostały utworzone dla usług.

Określanie folderu współdzielonego

Podczas instalacji Serwera administracyjnego możesz określić lokalizację folderu współdzielonego. Określenie lokalizacji folderu współdzielonego jest także możliwe po instalacji, we właściwościach Serwera administracyjnego. Domyślnie folder współdzielony zostanie utworzony na urządzeniu z zainstalowanym Serwerem administracyjnym (z uprawnieniami do odczytu dla podgrupy **Wszyscy**). Jednakże w niektórych przypadkach (takich, jak duże obciążenie sieci, konieczność uzyskania dostępu z odizolowanej sieci) przydatne może być umiejscowienie folderu współdzielonego w dedykowanym zasobie plików.

Folder współdzielony jest sporadycznie używany podczas instalacji Agenta sieciowego.

Uwzględnianie wielkości liter dla folderu współdzielonego musi być wyłączone.

Zdalna instalacja przy użyciu narzędzi Serwera administracyjnego poprzez profile grupy Active Directory

Jeśli urządzenia docelowe znajdują się w domenie systemu Windows (bez grup roboczych), wstępna zdalna instalacja (Agenta sieciowego i aplikacji zabezpieczającej na urządzeniach, które nie są jeszcze zarządzane) musi zostać przeprowadzona poprzez profile grupy Active Directory. Instalacja odbywa się przy użyciu standardowego zadania zdalnej instalacji z programu Kaspersky Security Center. W przypadku sieci dużej skali, dobrym rozwiązaniem jest umieszczenie folderu współdzielonego w dedykowanym zasobie plików w celu zmniejszenia obciążenia podsystemu dyskowego urządzenia z Serwerem administracyjnym.

Zdalna instalacja poprzez dostarczenie ścieżki UNC do pakietu autonomicznego

Jeśli użytkownicy urządzeń w sieci organizacji posiadają uprawnienia administratora lokalnego, stosowana jest inna metoda wstępnej instalacji - poprzez utworzenie autonomicznego pakietu Agenta sieciowego (lub nawet pakietu Agenta sieciowego połączonego z aplikacją zabezpieczającą). Po utworzeniu pakietu autonomicznego, należy wysłać do użytkowników odsyłacz do tego pakietu, który jest przechowywany w folderze współdzielonym. Instalacja rozpocznie się w momencie, gdy użytkownik kliknie odsyłacz.

Aktualizowanie z folderu współdzielonego Serwera administracyjnego

W zadaniu aktualizacji aplikacji antywirusowej możesz skonfigurować aktualizację z folderu współdzielonego Serwera administracyjnego. Jeśli zadanie zostało przypisane do dużej liczby urządzeń, dobrym rozwiązaniem będzie umieszczenie folderu współdzielonego w dedykowanym zasobie plików.

Instalowanie obrazów systemów operacyjnych

Obrazy systemu operacyjnego są zawsze instalowane poprzez folder współdzielony: urządzenia sczytują obrazy systemu operacyjnego z folderu współdzielonego. Jeśli instalacja obrazów została zaplanowana na dużej liczbie urządzeń firmowych, dobrym rozwiązaniem będzie umieszczenie folderu współdzielonego w dedykowanym zasobie plików.

Określanie adresu Serwera administracyjnego

Podczas instalacji Serwera administracyjnego możesz określić adres Serwera administracyjnego. Podczas tworzenia pakietów instalacyjnych Agenta sieciowego ten adres będzie używany jako domyślny.

Jako adres Serwera administracyjnego możesz określić:

- Nazwę NetBIOS Serwera administracyjnego, która jest określona domyślnie
- W pełni kwalifikowana nazwa domeny (FQDN) Serwera administracyjnego, jeśli system nazw domen (DNS) w sieci organizacji został skonfigurowany i działa poprawnie
- Adres zewnętrzny, jeśli Serwer administracyjny jest zainstalowany w strefie zdemilitaryzowanej (DMZ)

Wówczas możliwa będzie zmiana adresu Serwera administracyjnego przy użyciu narzędzi Konsoli administracyjnej; adres nie zostanie zmieniony automatycznie w już utworzonych pakietach instalacyjnych Agenta sieciowego.

Instalacja standardowa

Standardowa instalacja to instalacja Serwera administracyjnego, która używa domyślnych ścieżek dostępu dla plików aplikacji, instaluje domyślny zestaw wtyczek i nie włącza Zarządzania urządzeniami mobilnymi.

W celu zainstalowania Serwera administracyjnego Kaspersky Security Center na urządzeniu lokalnym:

Uruchom plik wykonywalny ksc_<numer wersji>.<numer kompilacji>_full_<wersja językowa>.exe.

Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Instaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Przeglądanie treści Umowy licencyjnej i Polityki prywatności

W tym kroku kreatora instalacji należy przeczytać Umowę licencyjną zawieraną między Tobą a firmą Kaspersky, a także Politykę prywatności.

Zaoferowane zostanie także przejrzenie Umów licencyjnych i Polityk prywatności dla wtyczek zarządzających aplikacjami, dostępnych w pakiecie dystrybucyjnym Kaspersky Security Center.

Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności, potwierdź to, zaznaczając odpowiednie pola wyboru.

Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

Krok 2. Wybieranie metody instalacji

W oknie wyboru typu instalacji wybierz **Standardowa**.

Instalacja standardowa jest zalecana, jeśli chcesz wypróbować Kaspersky Security Center, na przykład, poprzez przetestowanie działania aplikacji w małym obszarze wewnątrz sieci firmowej. Podczas instalacji standardowej konfigurujesz tylko bazę danych. Nie określasz żadnych ustawień Serwera administracyjnego - używane są wartości domyślne. W instalacji standardowej nie ma możliwości wybrania wtyczek zarządzających do zainstalowania; instalowany jest tylko domyślny zestaw wtyczek. Podczas instalacji standardowej nie są tworzone pakiety instalacyjne dla urządzeń mobilnych. Jednakże możesz utworzyć je później w Konsoli administracyjnej.

Krok 3. Instalowanie Kaspersky Security Center Web Console

Ten krok jest wyświetlany tylko wtedy, gdy korzystasz z 64-bitowego systemu operacyjnego. W przeciwnym wypadku ten krok nie jest wyświetlany, ponieważ Kaspersky Security Center Web Console nie działa z 32-bitowymi systemami operacyjnymi.

Domyślnie zostanie zainstalowana zarówno konsola Kaspersky Security Center Web Console, jak i Konsola administracyjna oparta na MMC.

Jeśli chcesz zainstalować tylko Kaspersky Security Center Web Console:

1. Wybierz **Zainstaluj tylko tę**.
2. Z listy rozwijalnej wybierz **Konsola internetowa**.

Instalacja Kaspersky Security Center Web Console rozpocznie się automatycznie po zakończeniu instalacji Serwera administracyjnego.

Jeśli chcesz zainstalować tylko konsolę opartą na MMC:

1. Wybierz **Zainstaluj tylko tę**.
2. Z listy rozwijalnej wybierz **Konsola oparta na MMC**.

Krok 4. Wybieranie rozmiaru sieci

Określ rozmiar sieci, w której instalowany jest Kaspersky Security Center. W zależności od liczby urządzeń w sieci, kreator odpowiednio konfiguruje instalację i wygląd interfejsu aplikacji.

Poniższa tabela wymienia ustawienia instalacyjne aplikacji i ustawienia wyglądu interfejsu, w zależności od różnych rozmiarów sieci.

Zależność ustawień instalacji od wybranej skali sieci

Ustawienia	1—100 urządzeń	101—1000 urządzeń	1000—5000 urządzeń	Więcej niż 5000 urządzeń
Wyświetlanie w drzewie konsoli węzłów podrzędnych i wirtualnych Serwerów administracyjnych oraz wszystkich ustawień związanych z podrzędnymi i wirtualnymi Serwerami administracyjnymi	Niedostępne	Niedostępne	Dostępne	Dostępne
Wyświetlanie sekcji **Zabezpieczenia** w oknach właściwości Serwera administracyjnego i grup administracyjnych	Niedostępne	Niedostępne	Dostępne	Dostępne
Losowy czas uruchomienia dla zadania aktualizacji na urządzeniach klienckich	Niedostępne	Ponad 5 minut	Ponad 10 minut	Ponad 10 minut

Jeśli łączysz Serwer administracyjny z serwerem bazodanowym MySQL 5.7 lub SQL Express, nie jest zalecane zarządzanie przy pomocy aplikacji liczbą urządzeń większą niż 10 000. W przypadku systemu zarządzania bazą danych MariaDB maksymalna zalecana liczba zarządzanych urządzeń to 20 000.

Krok 5. Wybieranie bazy danych

W tym kroku kreatora wybierz jeden z następujących systemów zarządzania bazami danych (DBMS), który będzie używany do przechowywania bazy danych Serwera administracyjnego:

- **Microsoft SQL Server lub SQL Server Express**
- **MySQL lub MariaDB**
- **PostgreSQL lub Postgres Pro**

Zaleca się zainstalowanie Serwera administracyjnego na serwerze dedykowanym zamiast na kontrolerze domeny. Jeśli instalujesz Kaspersky Security Center na serwerze, który działa jako kontroler domeny tylko do odczytu (RODC), Microsoft SQL Server (SQL Express) nie może zostać zainstalowany lokalnie (na tym samym urządzeniu). W tym przypadku zalecane jest zdalne zainstalowanie Microsoft SQL Server (SQL Express) (na innym urządzeniu) lub tego, którego używasz — MySQL, MariaDB, lub PostgreSQL — jeśli musisz zainstalować system DBMS lokalnie.

Struktura bazy danych Serwera administracyjnego jest opisana w pliku klakdb.chm, umieszczonym w folderze instalacyjnym Kaspersky Security Center. Ten plik jest również dostępny w archiwum w portalu Kaspersky: klakdb.zip.

Krok 6. Konfigurowanie serwera SQL

W tym kroku kreatora określ następujące ustawienia połączenia, w zależności od wybranego systemu zarządzania bazą danych (DBMS):

- Jeśli w poprzednim kroku wybrałeś **Microsoft SQL Server lub SQL Server Express**:
  - W polu **Nazwa instancji serwera SQL** określ nazwę serwera SQL w sieci. Aby wyświetlić listę wszystkich serwerów SQL, które są w sieci, kliknij przycisk **Przeglądaj**. Domyślnie to pole jest puste.

    Jeśli nawiążesz połączenie z serwerem SQL za pośrednictwem portu niestandardowego, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    Nazwa_hosta_serwera_SQL,1433
    ```

    Jeśli chronisz komunikację między Serwerem administracyjnym a serwerem SQL przy pomocy certyfikatu, w polu **Nazwa instancji serwera SQL** określ taką samą nazwę hosta, jaka była użyta w momencie generowania certyfikatu. Jeśli użyjesz nazwanej instancji serwera SQL, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    Nazwa_serwera_SQL,1433
    ```

    Jeśli używasz kilku instancji serwera SQL na tym samym hoście, wówczas dodatkowo określ nazwę instancji oddzieloną lewym ukośnikiem, na przykład:

    ```
    Nazwa_serwera_SQL\Nazwa_instancji_serwera_SQL,1433
    ```

    Jeśli serwer SQL w sieci firmowej ma włączoną funkcję Always On, określ nazwę odbiornika grupy dostępności w polu **Nazwa instancji serwera SQL**. Zauważ, że Serwer administracyjny obsługuje tylko tryb dostępności zatwierdzania synchronicznego, gdy włączona jest funkcja Always On.

  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

  Jeśli chcesz ręcznie zainstalować serwer SQL na urządzeniu, na którym instalujesz Kaspersky Security Center, będziesz musiał zatrzymać instalację i uruchomić ją ponownie po zainstalowaniu serwera SQL. Obsługiwane wersje serwerów SQL są wymienione w wymaganiach systemowych.

W przypadku, gdy ręcznie instalujesz serwer SQL na zdalnym urządzeniu, nie będzie potrzeby przerywania pracy kreatora instalacji Kaspersky Security Center. Zainstaluj serwer SQL i wznów instalację Kaspersky Security Center.

- Jeśli w poprzednim kroku wybrano **MySQL lub MariaDB**:
  - W polu **Nazwa instancji serwera SQL** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.
  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 3306.
  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.
- Jeśli w poprzednim kroku wybrano **Postgres**:
  - W polu **Nazwa instancji serwera Postgres** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.
  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 5432.
  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

Krok 7. Wybieranie trybu uwierzytelniania

Określ tryb uwierzytelniania, który będzie używany, gdy Serwer administracyjny połączy się z systemem zarządzania bazami danych (DBMS).

W zależności od wybranego DBMS, możesz wybrać jeden z następujących trybów uwierzytelniania:

- Dla SQL Express lub Microsoft SQL Server wybierz jedną z następujących opcji:
  - **Tryb uwierzytelniania Microsoft Windows**. Weryfikacja uprawnień wykorzystuje konto używane do uruchamiania Serwera administracyjnego.
  - **Tryb uwierzytelniania serwera SQL**. Jeśli wybierzesz tę opcję, do weryfikacji uprawnień zostanie użyte konto określone w oknie. Wypełnij pola **Konto** i **Hasło**.

    Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

  W przypadku obu trybów uwierzytelniania aplikacja sprawdza, czy baza danych jest dostępna. Jeśli baza danych nie jest dostępna, zostanie wyświetlony komunikat o błędzie, a Ty będziesz musiał dostarczyć poprawne dane uwierzytelniające.

  > Jeśli baza danych Serwera administracyjnego jest przechowywana na innym urządzeniu, a konto Serwera administracyjnego nie ma uprawnień dostępu do serwera bazy danych, podczas instalowania lub aktualizowania Serwera administracyjnego musisz użyć trybu uwierzytelniania serwera SQL. Może to mieć miejsce, gdy urządzenie przechowujące bazę danych znajduje się poza domeną lub gdy Serwer administracyjny jest instalowany z poziomu konta SystemLokalny.

- W przypadku MySQL, MariaDB, PostgreSQL lub Postgres Pro określ konto i hasło.

Krok 8. Wypakowywanie i instalowanie plików na dysku twardym

Po skonfigurowaniu instalacji modułów Kaspersky Security Center, możesz rozpocząć instalację plików na dysku twardym.

Jeśli instalacja wymaga dodatkowych programów, kreator instalacji powiadomi Cię o tym w oknie **Instalacja wymaganego oprogramowania** przed rozpoczęciem instalacji Kaspersky Security Center. Wymagane programy są instalowane automatycznie po kliknięciu przycisku **Dalej**.

W ostatnim kroku możesz wybrać, którą konsolę uruchomić do pracy z Kaspersky Security Center:

- **Uruchom Konsolę administracyjną MMC**
- **Uruchom Kaspersky Security Center Web Console**

  Ta opcja jest dostępna tylko wtedy, gdy w jednym z poprzednich kroków wybrano instalację Kaspersky Security Center Web Console.

Możesz także kliknąć **Zakończ**, aby zamknąć kreator bez rozpoczynania pracy z Kaspersky Security Center. Możesz rozpocząć pracę później w dowolnym momencie.

Przy pierwszym uruchomieniu Konsoli administracyjnej lub Kaspersky Security Center Web Console możesz przeprowadzić wstępną konfigurację aplikacji.

Po zakończeniu pracy kreatora instalacji, na dysku twardym są instalowane następujące moduły aplikacji:

- Serwer administracyjny (wraz z serwerową wersją Agenta sieciowego)
- Konsola administracyjna oparta na konsoli Microsoft Management Console
- Kaspersky Security Center Web Console (jeśli wybrano na instalację)
- Wtyczki do zarządzania aplikacjami dostępne w pakiecie dystrybucyjnym

Dodatkowo, zostanie zainstalowany Microsoft Windows Installer 4.5, jeśli nie był wcześniej zainstalowany.

Instalacja niestandardowa

Instalacja niestandardowa to instalacja Serwera administracyjnego, w trakcie której zostaniesz poproszony o wybranie składników, które mają zostać zainstalowane, i określenie folderu, w którym aplikacja ma zostać zainstalowana.

Korzystając z tego typu instalacji, możesz skonfigurować bazę danych i Serwer administracyjny, a także zainstalować składniki, które nie znajdują się w instalacji standardowej, lub wtyczki administracyjne dla różnych aplikacji zabezpieczających firmy Kaspersky. Możesz także włączyć Zarządzanie urządzeniami mobilnymi.

W celu zainstalowania Serwera administracyjnego Kaspersky Security Center na urządzeniu lokalnym:

Uruchom plik wykonywalny ksc_<numer wersji>.<numer kompilacji>_full_<wersja językowa>.exe.

Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Instaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Przeglądanie treści Umowy licencyjnej i Polityki prywatności

W tym kroku kreatora instalacji należy przeczytać Umowę licencyjną zawieraną między Tobą a firmą Kaspersky, a także Politykę prywatności.

Zaoferowane zostanie także przejrzenie Umów licencyjnych i Polityk prywatności dla wtyczek zarządzających aplikacjami, dostępnych w pakiecie dystrybucyjnym Kaspersky Security Center.

Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności, potwierdź to, zaznaczając odpowiednie pola wyboru.

Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

Krok 2. Wybieranie metody instalacji

W oknie wyboru typu instalacji określ **Niestandardowa**.

W instalacji niestandardowej możliwe jest zmodyfikowanie ustawień Kaspersky Security Center, takich jak: ścieżka dostępu do folderu współdzielonego, konta i porty dla połączenia z Serwerem administracyjnym oraz ustawienia bazy danych. Instalacja niestandardowa umożliwia określenie, które wtyczki zarządzające Kaspersky mają zostać zainstalowane. Podczas instalacji niestandardowej możesz utworzyć pakiety instalacyjne dla urządzeń mobilnych, włączając odpowiednią opcję.

Krok 3. Wybieranie składników do zainstalowania

Wybierz moduły Serwera administracyjnego Kaspersky Security Center, które chcesz zainstalować:

- **Zarządzanie urządzeniami mobilnymi**. Zaznacz to pole, jeśli musisz utworzyć pakiety instalacyjne dla urządzeń mobilnych, gdy uruchomiony jest kreator instalacji Kaspersky Security Center. Możesz także ręcznie utworzyć pakiety instalacyjne dla urządzeń mobilnych, po zainstalowaniu Serwera administracyjnego, korzystając z narzędzi Konsoli administracyjnej.

- **Agent SNMP**. Składnik ten pobiera dane statystyczne dla Serwera administracyjnego za pośrednictwem protokołu SNMP. Moduł jest dostępny tylko wtedy, gdy aplikacja jest instalowana na urządzeniu, na którym zainstalowany jest SNMP.

  Po zainstalowaniu Kaspersky Security Center, pliki .mib, potrzebne do zbierania danych statystycznych, zostaną umieszczone w podfolderze SNMP folderu instalacyjnego aplikacji.

Agent sieciowy i Konsola administracyjna nie są wyświetlane na liście modułów. Moduły te są instalowane automatycznie, nie możesz anulować ich instalacji.

W tym kroku musisz określić folder instalacyjny komponentów Serwera administracyjnego. Domyślnie moduły są instalowane w folderze <Dysk>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji. Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

Krok 4. Instalowanie Kaspersky Security Center Web Console

Ten krok jest wyświetlany tylko wtedy, gdy korzystasz z 64-bitowego systemu operacyjnego. W przeciwnym wypadku ten krok nie jest wyświetlany, ponieważ Kaspersky Security Center Web Console nie działa z 32-bitowymi systemami operacyjnymi.

Domyślnie zostanie zainstalowana zarówno konsola Kaspersky Security Center Web Console, jak i Konsola administracyjna oparta na MMC.

Jeśli chcesz zainstalować tylko Kaspersky Security Center Web Console:

1. Wybierz **Zainstaluj tylko tę**.
2. Z listy rozwijalnej wybierz **Konsola internetowa**.

Instalacja Kaspersky Security Center Web Console rozpocznie się automatycznie po zakończeniu instalacji Serwera administracyjnego.

Jeśli chcesz zainstalować tylko konsolę opartą na MMC:

1. Wybierz **Zainstaluj tylko tę**.
2. Z listy rozwijalnej wybierz **Konsola oparta na MMC**.

Krok 5. Wybieranie rozmiaru sieci

Określ rozmiar sieci, w której instalowany jest Kaspersky Security Center. W zależności od liczby urządzeń w sieci, kreator odpowiednio konfiguruje instalację i wygląd interfejsu aplikacji.

Poniższa tabela wymienia ustawienia instalacyjne aplikacji i ustawienia wyglądu interfejsu, w zależności od różnych rozmiarów sieci.

Zależność ustawień instalacji od wybranej skali sieci

Ustawienia	1—100 urządzeń	101—1000 urządzeń	1000—5000 urządzeń	Więcej niż 5000 urządzeń
Wyświetlanie w drzewie konsoli węzłów podrzędnych i wirtualnych Serwerów administracyjnych oraz wszystkich ustawień związanych z podrzędnymi i wirtualnymi Serwerami administracyjnymi	Niedostępne	Niedostępne	Dostępne	Dostępne
Wyświetlanie sekcji **Zabezpieczenia** w oknach właściwości Serwera administracyjnego i grup	Niedostępne	Niedostępne	Dostępne	Dostępne

administracyjnych				
Losowy czas uruchomienia dla zadania aktualizacji na urządzeniach klienckich	Niedostępne	Ponad 5 minut	Ponad 10 minut	Ponad 10 minut

Jeśli łączysz Serwer administracyjny z serwerem bazodanowym MySQL 5.7 lub SQL Express, nie jest zalecane zarządzanie przy pomocy aplikacji liczbą urządzeń większą niż 10 000. W przypadku systemu zarządzania bazą danych MariaDB maksymalna zalecana liczba zarządzanych urządzeń to 20 000.

Krok 6. Wybieranie bazy danych

W tym kroku kreatora wybierz jeden z następujących systemów zarządzania bazami danych (DBMS), który będzie używany do przechowywania bazy danych Serwera administracyjnego:

- **Microsoft SQL Server lub SQL Server Express**
- **MySQL lub MariaDB**
- **PostgreSQL lub Postgres Pro**

Zaleca się zainstalowanie Serwera administracyjnego na serwerze dedykowanym zamiast na kontrolerze domeny. Jeśli instalujesz Kaspersky Security Center na serwerze, który działa jako kontroler domeny tylko do odczytu (RODC), Microsoft SQL Server (SQL Express) nie może zostać zainstalowany lokalnie (na tym samym urządzeniu). W tym przypadku zalecane jest zdalne zainstalowanie Microsoft SQL Server (SQL Express) (na innym urządzeniu) lub tego, którego używasz — MySQL, MariaDB, lub PostgreSQL — jeśli musisz zainstalować system DBMS lokalnie.

Struktura bazy danych Serwera administracyjnego jest opisana w pliku klakdb.chm, umieszczonym w folderze instalacyjnym Kaspersky Security Center. Ten plik jest również dostępny w archiwum w portalu Kaspersky: klakdb.zip.

Krok 7. Konfigurowanie serwera SQL

W tym kroku kreatora określ następujące ustawienia połączenia, w zależności od wybranego systemu zarządzania bazą danych (DBMS):

- Jeśli w poprzednim kroku wybrałeś **Microsoft SQL Server lub SQL Server Express**:
  - W polu **Nazwa instancji serwera SQL** określ nazwę serwera SQL w sieci. Aby wyświetlić listę wszystkich serwerów SQL, które są w sieci, kliknij przycisk **Przeglądaj**. Domyślnie to pole jest puste.

    Jeśli nawiążesz połączenie z serwerem SQL za pośrednictwem portu niestandardowego, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    Nazwa_hosta_serwera_SQL,1433
    ```

    Jeśli chronisz komunikację między Serwerem administracyjnym a serwerem SQL przy pomocy certyfikatu, w polu **Nazwa instancji serwera SQL** określ taką samą nazwę hosta, jaka była użyta w momencie generowania certyfikatu. Jeśli użyjesz nazwanej instancji serwera SQL, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    Nazwa_serwera_SQL,1433
    ```

Jeśli używasz kilku instancji serwera SQL na tym samym hoście, wówczas dodatkowo określ nazwę instancji oddzieloną lewym ukośnikiem, na przykład:

```
Nazwa_serwera_SQL\Nazwa_instancji_serwera_SQL,1433
```

Jeśli serwer SQL w sieci firmowej ma włączoną funkcję Always On, określ nazwę odbiornika grupy dostępności w polu **Nazwa instancji serwera SQL**. Zauważ, że Serwer administracyjny obsługuje tylko tryb dostępności zatwierdzania synchronicznego, gdy włączona jest funkcja Always On.

- W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

Jeśli chcesz ręcznie zainstalować serwer SQL na urządzeniu, na którym instalujesz Kaspersky Security Center, będziesz musiał zatrzymać instalację i uruchomić ją ponownie po zainstalowaniu serwera SQL. Obsługiwane wersje serwerów SQL są wymienione w wymaganiach systemowych.

W przypadku, gdy ręcznie instalujesz serwer SQL na zdalnym urządzeniu, nie będzie potrzeby przerywania pracy kreatora instalacji Kaspersky Security Center. Zainstaluj serwer SQL i wznów instalację Kaspersky Security Center.

- Jeśli w poprzednim kroku wybrano **MySQL lub MariaDB**:
  - W polu **Nazwa instancji serwera SQL** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.
  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 3306.
  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.
- Jeśli w poprzednim kroku wybrano **Postgres**:
  - W polu **Nazwa instancji serwera Postgres** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.
  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 5432.
  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

Krok 8. Wybieranie trybu uwierzytelniania

Określ tryb uwierzytelniania, który będzie używany, gdy Serwer administracyjny połączy się z systemem zarządzania bazami danych (DBMS).

W zależności od wybranego DBMS, możesz wybrać jeden z następujących trybów uwierzytelniania:

- Dla SQL Express lub Microsoft SQL Server wybierz jedną z następujących opcji:
  - **Tryb uwierzytelniania Microsoft Windows**. Weryfikacja uprawnień wykorzystuje konto używane do uruchamiania Serwera administracyjnego.
  - **Tryb uwierzytelniania serwera SQL**. Jeśli wybierzesz tę opcję, do weryfikacji uprawnień zostanie użyte konto określone w oknie. Wypełnij pola **Konto** i **Hasło**.

    Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

W przypadku obu trybów uwierzytelniania aplikacja sprawdza, czy baza danych jest dostępna. Jeśli baza danych nie jest dostępna, zostanie wyświetlony komunikat o błędzie, a Ty będziesz musiał dostarczyć poprawne dane uwierzytelniające.

Jeśli baza danych Serwera administracyjnego jest przechowywana na innym urządzeniu, a konto Serwera administracyjnego nie ma uprawnień dostępu do serwera bazy danych, podczas instalowania lub aktualizowania Serwera administracyjnego musisz użyć trybu uwierzytelniania serwera SQL. Może to mieć miejsce, gdy urządzenie przechowujące bazę danych znajduje się poza domeną lub gdy Serwer administracyjny jest instalowany z poziomu konta SystemLokalny.

- W przypadku MySQL, MariaDB, PostgreSQL lub Postgres Pro określ konto i hasło.

Krok 9. Wybieranie konta do uruchamiania Serwera administracyjnego

Wybierz konto, z poziomu którego Serwer administracyjny będzie uruchamiany jako usługa.

- **Utwórz konto automatycznie**. Aplikacja tworzy konto pod nazwą KL-AK-*, z którego zostanie uruchomiona usługa kladminserver.

  Możesz wybrać tę opcję, jeśli planujesz umieścić folder współdzielony i DBMS na tym samym urządzeniu co Serwer administracyjny.

- **Wybierz konto**. Usługa Serwera administracyjnego (kladminserver) zostanie uruchomiona z poziomu konta, które wybrałeś.

  Będziesz musiał wybrać konto domenowe, jeśli, na przykład, planujesz używać DBMS jako instancji serwera SQL w dowolnej wersji, w tym SQL Express, który znajduje się na innym urządzeniu, i/lub planujesz umieścić folder współdzielony na innym urządzeniu.

  Kaspersky Security Center obsługuje zarządzane konta usługi (MSA) i grupę zarządzanych kont usługi (gMSA). Jeśli w Twojej domenie używane są tego typu konta, możesz wybrać jedno z nich jako konto dla usługi Serwera administracyjnego.

  Przed określeniem MSA lub gMSA musisz zainstalować konto na tym samym urządzeniu, na którym chcesz zainstalować serwer administracyjny. Jeśli konto nie zostało jeszcze zainstalowane, anuluj instalację Serwera administracyjnego, zainstaluj konto, a następnie uruchom ponownie instalację Serwera administracyjnego. Szczegółowe informacje na temat instalacji zarządzanych kont usług na urządzeniu lokalnym można znaleźć w oficjalnej dokumentacji firmy Microsoft.

  Aby określić MSA lub gMSA:

  1. Kliknij przycisk **Przeglądaj**.
  2. W otwartym oknie kliknij przycisk **Typ obiektu**.
  3. Wybierz typ **Konto dla usług** i kliknij **OK**.
  4. Wybierz odpowiednie konto i kliknij **OK**.

Wybrane konto musi posiadać różne uprawnienia, w zależności od systemu DBMS, którego planujesz używać.

W celach bezpieczeństwa nie należy przydzielać stanu uprzywilejowanego do konta, z poziomu którego uruchamiasz Serwer administracyjny.

Jeżeli w przyszłości będziesz chciał zmienić konto Serwera administracyjnego, będziesz mógł użyć narzędzia do przełączania konta Serwera administracyjnego (klsrvswch).

Krok 10. Wybieranie konta do uruchamiania usług Kaspersky Security Center

Wybierz konto, z poziomu którego usługi Kaspersky Security Center będą uruchomione na tym urządzeniu:

- **Utwórz konto automatycznie**. Kaspersky Security Center tworzy lokalne konto o nazwie KlScSvc na tym urządzeniu w grupie kladmins. Usługi Kaspersky Security Center zostaną uruchomione z poziomu utworzonego konta.

- **Wybierz konto**. Usługi Kaspersky Security Center będą uruchamiane z poziomu wybranego konta.

  Będziesz musiał wybrać konto domenowe, jeśli, na przykład, planujesz zapisywać raporty do folderu znajdującego się na innym urządzeniu lub jeśli jest to wymagane przez politykę bezpieczeństwa organizacji. Konieczne może być także wybranie konta domeny, jeśli instalujesz Serwer administracyjny na klastrze typu failover.

W celach bezpieczeństwa nie należy przydzielać stanu uprzywilejowanego do konta, z poziomu którego uruchamiane są usługi.

Usługa KSN proxy (ksnproxy), usługa Kaspersky activation proxy (klactprx) oraz usługa Kaspersky authentication portal (klwebsrv) będą uruchamiane z poziomu wybranego konta.

Krok 11. Wybieranie folderu współdzielonego

Określ lokalizację i nazwę foldera współdzielonego, który będzie wykorzystywany do następujących zadań:

- Przechowywania plików potrzebnych do przeprowadzenia zdalnej instalacji aplikacji (te pliki są kopiowanie na Serwer administracyjny podczas tworzenia pakietów instalacyjnych).

- Przechowywania uaktualnień pobranych ze źródła uaktualnień na Serwer administracyjny.

Współdzielenie plików (tylko do odczytu) będzie możliwe dla wszystkich użytkowników.

Możesz wybrać jedną z następujących opcji:

- **Utwórz folder współdzielony**. Utwórz nowy folder. W polu do wprowadzenia tekstu określ ścieżkę dostępu do folderu.

- **Wskaż istniejący folder współdzielony**. Wybierz folder współdzielony, który już istnieje.

Folder współdzielony może być folderem lokalnym na urządzeniu, które jest używane do instalacji, lub zdalnym folderem na dowolnym urządzeniu klienckim w obrębie sieci firmowej. Folder współdzielony można wybrać przez kliknięcie przycisku **Przeglądaj** lub ręczne wprowadzenie jego ścieżki w formacie UNC (na przykład \\server\Share) w odpowiednim polu.

Domyślnie instalator tworzy lokalny podfolder Share w folderze aplikacji zawierającym moduły Kaspersky Security Center.

W razie potrzeby folder udostępniony można zdefiniować później.

Krok 12. Konfigurowanie połączenia z Serwerem administracyjnym

Skonfiguruj połączenie z Serwerem administracyjnym:

- **Port**

  Numer portu używanego do nawiązywania połączenia z Serwerem administracyjnym.

  Domyślny numer portu to 14000.

- **Port SSL**

  Numer portu Secure Sockets Layer (SSL) używanego do nawiązywania bezpiecznego połączenia z Serwerem administracyjnym poprzez SSL.

  Domyślny numer portu to 13000.

- **Długość klucza szyfrowania**

  Wybierz długość klucza szyfrowania: 1024 bity lub 2048 bitów.

  Klucz szyfrowania o długości 1024 bitów w mniejszym stopniu obciąża procesor, ale jest uznawany za przestarzały, ponieważ nie zapewnia niezawodnego szyfrowania ze względu na swoją specyfikację techniczną. Dodatkowo, istniejący sprzęt okaże się niekompatybilny z certyfikatami SSL zawierającymi 1024-bitowe klucze.

  Klucz szyfrowania o długości 2048 bitów spełnia wszystkie najnowocześniejsze standardy szyfrowania. Jednakże użycie 2048-bitowego klucza szyfrowania może zwiększyć obciążenie procesora.

  Domyślnie wybrana jest opcja **2048 bitów (największe bezpieczeństwo)**.

Jeżeli Serwer administracyjny jest zainstalowany na urządzeniu działającym pod kontrolą systemu Microsoft Windows XP Service Pack 2, wówczas wbudowana zapora sieciowa będzie blokowała porty TCP: 13000 i 14000. Dlatego też, aby zezwolić na dostęp do Serwera administracyjnego na urządzeniu po instalacji, należy ręcznie otworzyć te porty.

Krok 13. Określanie adresu Serwera administracyjnego

Określ adres Serwera administracyjnego przy użyciu jednej z następujących metod:

- **Nazwa domeny DNS**. Metoda ta jest użyteczna, gdy sieć zawiera serwer DNS, którego urządzenia klienckie mogą użyć do uzyskania adresu Serwera administracyjnego.
- **Nazwa NetBIOS**. Metoda ta jest przydatna, gdy urządzenia klienckie uzyskują adres Serwera administracyjnego za pośrednictwem protokołu NetBIOS lub gdy w sieci dostępny jest serwer WINS.
- **Adres IP**. Metoda ta jest używana, gdy Serwer administracyjny posiada stały adres IP, który w przyszłości nie zostanie zmieniony.

Jeśli zainstalowano Kaspersky Security Center na aktywnym węźle klastra pracy trybu failover Kaspersky i podczas przygotowania węzłów klastra utworzona została wirtualna karta sieciowa, określ adres IP tej karty. W przeciwnym razie wpisz adres IP modułu równoważenia obciążenia innej firmy, którego używasz.

Krok 14. Adres Serwera administracyjnego dla podłączenia urządzeń mobilnych

Ten krok kreatora instalacji jest dostępny, jeśli moduł Zarządzanie urządzeniami mobilnymi został wybrany do zainstalowania.

W oknie **Adres do podłączenia urządzeń mobilnych** określ zewnętrzny adres Serwera administracyjnego dla podłączenia urządzeń mobilnych, które znajdują się poza siecią lokalną. Możesz określić adres IP lub system nazw domen (DNS) Serwera administracyjnego.

Krok 15. Wybieranie wtyczek do zarządzania aplikacjami

Wybierz wtyczki zarządzające aplikacjami, które mają być zainstalowane wraz z Kaspersky Security Center.

Aby ułatwić wyszukiwanie, wtyczki są podzielone na grupy w zależności od typu chronionych obiektów.

Krok 16. Wypakowywanie i instalowanie plików na dysku twardym

Po skonfigurowaniu instalacji modułów Kaspersky Security Center, możesz rozpocząć instalację plików na dysku twardym.

Jeśli instalacja wymaga dodatkowych programów, kreator instalacji powiadomi Cię o tym w oknie **Instalacja wymaganego oprogramowania** przed rozpoczęciem instalacji Kaspersky Security Center. Wymagane programy są instalowane automatycznie po kliknięciu przycisku **Dalej**.

W ostatnim kroku możesz wybrać, którą konsolę uruchomić do pracy z Kaspersky Security Center:

- **Uruchom Konsolę administracyjną MMC**
- **Uruchom Kaspersky Security Center Web Console**

  Ta opcja jest dostępna tylko wtedy, gdy w jednym z poprzednich kroków wybrano instalację Kaspersky Security Center Web Console.

Możesz także kliknąć **Zakończ**, aby zamknąć kreator bez rozpoczynania pracy z Kaspersky Security Center. Możesz rozpocząć pracę później w dowolnym momencie.

Przy pierwszym uruchomieniu Konsoli administracyjnej lub Kaspersky Security Center Web Console możesz przeprowadzić wstępną konfigurację aplikacji.

Wdrażanie klastra trybu failover Kaspersky

Ta sekcja zawiera zarówno ogólne informacje o klastrze trybu failover Kaspersky, jak i instrukcje dotyczące przygotowania i instalacji klastra trybu failover Kaspersky w Twojej sieci.

Scenariusz: Wdrażanie klastra trybu failover Kaspersky

Klaster trybu failover Kaspersky zapewnia wysoką dostępność Kaspersky Security Center i minimalizuje czas przestoju Serwera administracyjnego w przypadku awarii. Klaster trybu failover opiera się na dwóch identycznych instancjach Kaspersky Security Center, zainstalowanych na dwóch komputerach. Jedna z instancji pracuje jako węzeł aktywny, a druga jako węzeł pasywny. Węzeł aktywny zarządza ochroną urządzeń klienckich, natomiast węzeł pasywny jest przygotowany do przejęcia wszystkich funkcji węzła aktywnego w przypadku awarii węzła aktywnego. Gdy wystąpi awaria, węzeł pasywny staje się aktywny, a węzeł aktywny staje się pasywny.

Wymagania wstępne

Masz sprzęt spełniający wymagania dla klastra trybu failover.

Etapy

Wdrożenie aplikacji firmy Kaspersky odbywa się w krokach:

1. **Tworzenie konta dla usług Kaspersky Security Center**

   Utwórz nową grupę domen (w tym scenariuszu dla tej grupy jest używana nazwa 'KLAdmins'), a następnie nadaj grupie uprawnienia administratora lokalnego na obu węzłach i na serwerze plików. Następnie utwórz dwa nowe konta użytkowników domeny (w tym scenariuszu nazwy „ksc" i „rightless" są używane dla tych kont) i dodaj konta do grupy domeny KLAdmins.

   Dodaj konto użytkownika, pod którym zostanie zainstalowany Kaspersky Security Center, do wcześniej utworzonej grupy domeny KLAdmins.

2. **Przygotowanie serwera plików**

   Przygotuj serwer plików do pracy jako komponent klastra trybu failover Kaspersky. Upewnij się, że serwer plików spełnia wymagania sprzętowe i programowe, utwórz dwa foldery współdzielone dla danych Kaspersky Security Center i skonfiguruj uprawnienia dostępu do folderów współdzielonych.

   Instrukcje: Przygotowanie serwera plików dla klastra trybu failover Kaspersky

3. **Przygotowanie węzłów aktywnych i pasywnych**

   Przygotuj dwa komputery z identycznym sprzętem i oprogramowaniem do pracy jako węzły aktywne i pasywne.

   Instrukcje: Przygotowywanie węzłów dla klastra trybu failover Kaspersky

4. **Instalacja systemu zarządzania bazą danych (DBMS)**

   Wybierz dowolny z obsługiwanych systemów DBMS, a następnie zainstaluj DBMS na dedykowanym komputerze.

5. **Instalacja Kaspersky Security Center**

   Zainstaluj Kaspersky Security Center w klastrze trybu failover na obu węzłach. Najpierw musisz zainstalować Kaspersky Security Center na aktywnym węźle, a następnie zainstalować go na węźle pasywnym.

   Dodatkowo, możesz zainstalować Kaspersky Security Center Web Console na oddzielnym urządzeniu, które nie jest węzłem klastra.

   Instrukcje: Instalowanie Kaspersky Security Center na węzłach klastra trybu failover Kaspersky

6. **Testowanie klastra trybu failover**

   Sprawdź, czy poprawnie skonfigurowano klaster trybu failover i czy działa poprawnie. Na przykład, możesz zatrzymać jedną z usług Kaspersky Security Center na aktywnym węźle: kladminserver, klnagent, ksnproxy, klactprx lub klwebsrv. Po zatrzymaniu usługi zarządzanie ochroną musi zostać automatycznie przełączone na węzeł pasywny.

Wyniki

Wdrożony zostaje klaster trybu failover Kaspersky. Prosimy o zapoznanie się ze zdarzeniami, które prowadzą do przełączenia między aktywnym i pasywnym węzłem.

Informacje o klastrze trybu failover Kaspersky

Klaster trybu failover Kaspersky zapewnia wysoką dostępność Kaspersky Security Center i minimalizuje czas przestoju Serwera administracyjnego w przypadku awarii. Klaster trybu failover opiera się na dwóch identycznych instancjach Kaspersky Security Center, zainstalowanych na dwóch komputerach. Jedna z instancji pracuje jako węzeł aktywny, a druga jako węzeł pasywny. Węzeł aktywny zarządza ochroną urządzeń klienckich, natomiast węzeł pasywny jest przygotowany do przejęcia wszystkich funkcji węzła aktywnego w przypadku awarii węzła aktywnego. Gdy wystąpi awaria, węzeł pasywny staje się aktywny, a węzeł aktywny staje się pasywny.

Wymagania sprzętowe i programowe

W celu zainstalowania klastra trybu failover Kaspersky musisz mieć następujący sprzęt:

- Dwa komputery z identycznym sprzętem i oprogramowaniem. Te komputery będą działać jako węzły aktywne i pasywne.
- Serwer plików obsługujący protokół CIFS/SMB w wersji 2.0 lub nowszej. Musisz zapewnić dedykowany komputer, który będzie działał jako serwer plików.

  > Upewnij się, że zapewniłeś wysoką przepustowość sieci między serwerem plików a aktywnymi i pasywnymi węzłami.

- Komputer z systemem zarządzania bazami danych (DBMS).

Warunki przełączenia

Klaster trybu failover przełącza zarządzanie ochroną urządzeń klienckich z węzła aktywnego na węzeł pasywny, jeśli na węźle aktywnym wystąpi dowolne z następujących zdarzeń:

- Węzeł aktywny jest uszkodzony z powodu awarii oprogramowania lub sprzętu.
- Węzeł aktywny został tymczasowo zatrzymany na działania konserwacyjne.
- Przynajmniej jedna z usług (lub procesów) Kaspersky Security Center uległa awarii lub została celowo zamknięta przez użytkownika. Usługi Kaspersky Security Center są następujące: kladminserver, klnagent, klactprx i klwebsrv.

- Połączenie sieciowe między aktywnym węzłem a magazynem na serwerze plików zostało przerwane lub zakończone.

Przygotowywanie serwera plików dla klastra trybu failover Kaspersky

Serwer plików działa jako wymagany składnik klastra trybu failover Kaspersky.

W celu przygotowania serwera plików:

1. Upewnij się, że serwer plików spełnia wymagania sprzętowe i programowe.
2. Upewnij się, że serwer plików i oba węzły (aktywny i pasywny) znajdują się w tej samej domenie lub serwer plików jest kontrolerem domeny.
3. Na serwerze plików utwórz dwa foldery współdzielone. Jeden z nich służy do przechowywania informacji o klastrze trybu failover. Drugi służy do przechowywania danych i ustawień Kaspersky Security Center. Ścieżki do folderów współdzielonych określisz podczas konfigurowania instalacji Kaspersky Security Center.
4. Przyznaj pełne uprawnienia dostępu (zarówno uprawnienia udziału, jak i uprawnienia NTFS) do utworzonych folderów współdzielonych dla następujących kont użytkowników i grup:
   - Grupa domen KLAdmins.
   - Konta użytkowników $<node1> i $<node2>. W tym przypadku <node1> oraz <node2> to nazwy komputerów aktywnych i pasywnych węzłów.

Serwer plików jest przygotowany. Aby zainstalować klaster trybu failover Kaspersky, postępuj zgodnie z dalszymi instrukcjami w tym scenariuszu.

Przygotowywanie węzłów dla klastra trybu failover Kaspersky

Przygotuj dwa komputery do pracy jako węzły aktywne i pasywne dla klastra trybu failover Kaspersky.

W celu przygotowania węzłów dla klastra trybu failover Kaspersky:

1. Upewnij się, że masz dwa komputery, które spełniają wymagania sprzętowe i programowe. Te komputery będą działać jako aktywne i pasywne węzły klastra trybu failover.
2. Upewnij się, że serwer plików i oba węzły znajdują się w tej samej domenie.
3. Wykonaj jedną z poniższych czynności:
   - W każdym z węzłów utwórz wirtualną kartę sieciową. Możesz to zrobić za pomocą oprogramowania innej firmy.

     Upewnij się, że spełnione są następujące warunki:

     - Wirtualne karty sieciowe muszą być wyłączone. Wirtualne karty sieciowe można utworzyć w stanie wyłączonym lub wyłączyć je po utworzeniu.
     - Wirtualne karty sieciowe w obu węzłach muszą mieć ten sam adres IP.

- Użyj modułu równoważenia obciążenia innej firmy. Na przykład, możesz użyć serwera nginx. W takim przypadku wykonaj następujące czynności:

  a. Zapewnij dedykowany komputer oparty o system Linux z zainstalowanym nginx.

  b. Skonfiguruj moduł równoważenia obciążenia. Ustaw węzeł aktywny jako serwer główny, a węzeł pasywny jako serwer zapasowy.

  c. Na serwerze nginx otwórz wszystkie porty Serwera administracyjnego: TCP 13000, UDP 13000, TCP 13291, TCP 13299 i TCP 17000.

4. Uruchom ponownie oba węzły i serwer plików.

5. Zmapuj dwa foldery współdzielone, które utworzyłeś podczas kroku przygotowania serwera plików, do każdego z węzłów. Musisz zmapować foldery współdzielone jako dyski sieciowe. Podczas mapowania folderów możesz wybrać dowolne wolne litery dysków. Aby uzyskać dostęp do folderów współdzielonych, użyj poświadczeń konta użytkownika utworzonego w kroku 1 procedury scenariusza.

Węzły są przygotowane. Aby zainstalować klaster trybu failover Kaspersky, postępuj zgodnie z dalszymi instrukcjami scenariusza.

Instalowanie Kaspersky Security Center na węzłach klastra trybu failover Kaspersky

Kaspersky Security Center jest instalowany na obu węzłach klastra trybu failover Kaspersky oddzielnie. W pierwszej kolejności instalujesz aplikację na węźle aktywnym, a następnie na węźle pasywnym. Podczas instalacji wybierasz, który węzeł będzie aktywny, a który będzie pasywny.

Tylko użytkownik z grupy domen KLAdmins może zainstalować Kaspersky Security Center na każdym węźle.

W celu zainstalowania Kaspersky Security Center na aktywnym węźle klastra trybu failover Kaspersky:

1. Uruchom plik wykonywalny ksc_14.2_<numer kompilacji>_full_<wersja językowa>.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

2. Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się na wszystkie warunki Umowy licencyjnej i Polityki prywatności, w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących:** zaznacz następujące pola:

   - **Warunki i postanowienia tej Umowy licencyjnej**
   - **Politykę prywatności opisującą zasady przetwarzania danych**

   Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

   Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

3. Wybierz **Węzeł podstawowy klastra Kaspersky Failover**, aby zainstalować aplikację na aktywnym węźle.

4. W oknie **Folder współdzielony** wykonaj następujące czynności:

   - W polach **Udział stanu** i **Udział danych** określ ścieżki do folderów współdzielonych, które utworzyłeś na serwerze plików podczas jego przygotowania.
   - W polach **Dysk udziału stanu** i **Dysk udziału danych** wybierz dyski sieciowe, na które zmapowałeś foldery współdzielone podczas przygotowania węzłów.
   - Wybierz tryb łączności klastra: za pośrednictwem wirtualnej karty sieciowej lub modułu równoważenia obciążenia innej firmy.

5. Wykonaj inne kroki instalacji niestandardowej, zaczynając od kroku 3.

   W kroku 13 określ adres IP wirtualnej karty sieciowej, jeśli utworzyłeś kartę podczas przygotowania węzłów klastra. W przeciwnym razie wpisz adres IP modułu równoważenia obciążenia innej firmy, którego używasz.

Kaspersky Security Center jest zainstalowany na aktywnym węźle.

W celu zainstalowania Kaspersky Security Center na pasywnym węźle klastra trybu failover Kaspersky:

1. Uruchom plik wykonywalny ksc_14.2_<numer kompilacji>_full_<wersja językowa>.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

2. Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się na wszystkie warunki Umowy licencyjnej i Polityki prywatności, w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących:** zaznacz następujące pola:

   - **Warunki i postanowienia tej Umowy licencyjnej**
   - **Politykę prywatności opisującą zasady przetwarzania danych**

   Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

   Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

3. Wybierz **Węzeł pomocniczy klastra Kaspersky Failover**, aby zainstalować aplikację na pasywnym węźle.

4. W oknie **Folder współdzielony**, w polu **Udział stanu** podaj ścieżkę do folderu współdzielonego z informacjami o stanie klastra, który utworzyłeś na serwerze plików podczas jego przygotowania.

5. Kliknij przycisk **Zainstaluj**. Po zakończeniu instalacji kliknij przycisk **Finish**.

Kaspersky Security Center jest zainstalowany na pasywnym węźle. Teraz możesz przetestować klaster trybu failover Kaspersky, aby upewnić się, że został poprawnie skonfigurowany i działa poprawnie.

Ręczne uruchamianie i zatrzymywanie węzłów klastra

Konieczne może być zatrzymanie całego klastra trybu failover Kaspersky lub tymczasowe odłączenie jednego z węzłów klastra w celu konserwacji. W takim przypadku postępuj zgodnie z instrukcjami w tej sekcji. Nie próbuj uruchamiać ani zatrzymywać usług lub procesów związanych z klastrem trybu failover za pomocą innych środków. To może spowodować utratę danych.

Uruchamianie i zatrzymywanie całego klastra trybu failover w celu konserwacji

W celu uruchomienia lub zatrzymania całego klastra trybu failover:

1. Na aktywnym węźle przejdź do <Dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Otwórz wiersz polecenia, a następnie uruchom jedno z następujących poleceń:
   - Aby zatrzymać klaster, uruchom: `klfoc -stopcluster --stp klfoc`
   - Aby uruchomić klaster, uruchom: `klfoc -startcluster --stp klfoc`

Klaster trybu failover jest uruchamiany lub zatrzymywany w zależności od uruchomionego polecenia.

Utrzymywanie jednego z węzłów

W celu utrzymania jednego z węzłów:

1. W węźle aktywnym zatrzymaj klaster trybu failover, używając polecenia `klfoc -stopcluster --stp klfoc`.
2. W węźle, który chcesz poddać działaniom konserwacyjnym, przejdź do <Dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Otwórz wiersz poleceń, a następnie odłącz węzeł od klastra, uruchamiając polecenie `detach_node.cmd`.
4. W węźle aktywnym uruchom klaster trybu failover za pomocą polecenia `klfoc -startcluster --stp klfoc`.
5. Wykonaj działania konserwacyjne.
6. W węźle aktywnym zatrzymaj klaster trybu failover, używając polecenia `klfoc -stopcluster --stp klfoc`.
7. W węźle, na którym wykonywano działania konserwacyjne, przejdź do <Dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
8. Otwórz wiersz poleceń, a następnie dołącz węzeł do klastra, uruchamiając polecenie `attach_node.cmd`.
9. W węźle aktywnym uruchom klaster trybu failover za pomocą polecenia `klfoc -startcluster --stp klfoc`.

Węzeł jest utrzymywany i dołączany do klastra trybu failover.

Instalowanie Serwera administracyjnego na klastrze trybu failover Microsoft

Procedura instalacji Serwera administracyjnego w klastrze typu failover różni się zarówno od standardowej, jak i niestandardowej instalacji na urządzeniu autonomicznym.

Wykonaj procedurę opisaną w tej sekcji na węźle, który zawiera wspólny magazyn danych klastra.

W celu zainstalowania Serwera administracyjnego Kaspersky Security Center na klastrze:

Uruchom plik wykonywalny ksc_<numer wersji>.<numer kompilacji>_full_<wersja językowa>.exe.

Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania. W oknie wyboru aplikacji kliknij odnośnik **Instaluj Serwer administracyjny Kaspersky Security Center**, aby uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Przeglądanie treści Umowy licencyjnej i Polityki prywatności

W tym kroku kreatora instalacji należy przeczytać Umowę licencyjną zawieraną między Tobą a firmą Kaspersky, a także Politykę prywatności.

Zaoferowane zostanie także przejrzenie Umów licencyjnych i Polityk prywatności dla wtyczek zarządzających aplikacjami, dostępnych w pakiecie dystrybucyjnym Kaspersky Security Center.

Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności, potwierdź to, zaznaczając odpowiednie pola wyboru.

Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól.

Jeśli nie akceptujesz warunków Umowy licencyjnej lub Polityki prywatności, anuluj instalację, klikając przycisk **Anuluj**.

Krok 2. Wybieranie typu instalacji na klastrze

Wybierz typ instalacji na klastrze:

- **Klaster (zainstaluj na wszystkich węzłach klastra)**

  To jest zalecana opcja. Jeśli wybierzesz tę opcję, Serwer administracyjny zostanie zainstalowany na wszystkich węzłach klastra jednocześnie.

  > Na etapie wyboru Konsoli administracyjnej do instalacji należy wybrać konsolę, która zostanie zainstalowana na bieżącym węźle klastra. Jeśli zainstalujesz konsolę tylko na węźle klastra, w przypadku awarii węzła utracisz dostęp do Serwera administracyjnego. Zalecamy, aby podczas tego kroku wybrać konsolę opartą na MMC do instalacji na wszystkich węzłach klastra. Po zainstalowaniu Serwera administracyjnego zainstaluj Kaspersky Security Center Web Console na oddzielnym urządzeniu, które nie jest węzłem klastra. Pozwala to na zarządzanie Serwerem administracyjnym przy użyciu Kaspersky Security Center Web Console, jeśli węzeł klastra ulegnie awarii.

- **Lokalnie (zainstaluj tylko na tym urządzeniu)**

Jeśli wybierzesz tę opcję, Serwer administracyjny zostanie zainstalowany tylko na bieżącym węźle, tak jak na serwerze autonomicznym, a Serwer administracyjny nie będzie działał jako aplikacja typu cluster-aware. Na przykład, możesz chcieć wybrać tę opcję, aby zaoszczędzić współdzieloną przestrzeń dyskową, jeśli odporność na uszkodzenia nie jest potrzebna dla Serwera administracyjnego. W przypadku awarii bieżącego węzła, będziesz musiał zainstalować Serwer administracyjny na innym węźle i przywrócić stan Serwera administracyjnego z kopii zapasowej.

Dalsze kroki są takie same, jak w przypadku standardowej lub niestandardowej metody instalacji, począwszy od kroku wyboru metody instalacji.

Krok 3. Określanie nazwy wirtualnego Serwera administracyjnego

Określ nazwę sieciową nowego wirtualnego Serwera administracyjnego. Będzie można użyć tej nazwy do połączenia Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console z Serwerem administracyjnym.

Określona nazwa musi różnić się od nazwy klastra.

Krok 4. Określanie szczegółów sieci wirtualnego Serwera administracyjnego

W celu określenia szczegółów sieci nowej instancji wirtualnego Serwera administracyjnego:

1. W sekcji **Sieć do użycia** wybierz sieć domeny, do której jest podłączony bieżący węzeł klastra.
2. Wykonaj jedną z poniższych czynności:
   - Jeśli w wybranej sieci, do przypisywania adresów IP używany jest protokół DHCP, wybierz opcję **Użyj DHCP**.
   - Jeśli w wybranej sieci nie jest używany protokół DHCP, określ wymagany adres IP.

     Podany adres IP musi różnić się od adresu IP klastra.
3. Kliknij **Dodaj**, aby zastosować określone ustawienia.

Będziesz mógł użyć automatycznie przypisanego lub określonego adresu IP do połączenia Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console z Serwerem administracyjnym.

Krok 5. Określanie grupy klastrów

Grupa klastrów to specjalny klaster typu failover, który zawiera wspólne zasoby dla wszystkich węzłów. Masz dwie opcje:

- Tworzenie nowej grupy klastrów.

  Ta opcja jest zalecana w większości przypadków. Nowa grupa klastrów będzie zawierać wszystkie wspólne zasoby związane z instancją Serwera administracyjnego.
- Wybieranie istniejącej grupy klastrów.

Wybierz tę opcję, jeśli chcesz użyć wspólnego zasobu, który jest już skojarzony z istniejącą grupą klastrów. Na przykład, możesz chcieć użyć tej opcji, jeśli chcesz użyć magazynu skojarzonego z istniejącą grupą klastrów i jeśli nie ma innego dostępnego magazynu dla nowej grupy klastrów.

Krok 6. Wybieranie magazynu danych klastra

W celu wybrania magazynu danych klastra:

1. W sekcji **Dostępne repozytoria** wybierz magazyn danych, w którym zostaną zainstalowane wspólne zasoby instancji wirtualnego Serwera administracyjnego.
2. Jeśli wybrany magazyn danych zawiera kilka woluminów, w sekcji **Dostępne sekcje na dysku twardym** wybierz wymagany wolumin.
3. W sekcji **Ścieżka instalacji** wprowadź ścieżkę do wspólnego magazynu danych, w którym zostaną zainstalowane zasoby instancji wirtualnego Serwera administracyjnego.

Magazyn danych został wybrany.

Krok 7. Określanie konta do zdalnej instalacji

Podaj nazwę użytkownika i hasło, które będą używane do zdalnej instalacji instancji wirtualnego Serwera administracyjnego w pasywnym węźle klastra.

Określone konto musi mieć nadane uprawnienia administracyjne na wszystkich węzłach klastra.

Krok 8. Wybieranie składników do zainstalowania

Wybierz moduły Serwera administracyjnego Kaspersky Security Center, które chcesz zainstalować:

- **Zarządzanie urządzeniami mobilnymi**. Zaznacz to pole, jeśli musisz utworzyć pakiety instalacyjne dla urządzeń mobilnych, gdy uruchomiony jest kreator instalacji Kaspersky Security Center. Możesz także ręcznie utworzyć pakiety instalacyjne dla urządzeń mobilnych, po zainstalowaniu Serwera administracyjnego, korzystając z narzędzi Konsoli administracyjnej.
- **Agent SNMP**. Składnik ten pobiera dane statystyczne dla Serwera administracyjnego za pośrednictwem protokołu SNMP. Moduł jest dostępny tylko wtedy, gdy aplikacja jest instalowana na urządzeniu, na którym zainstalowany jest SNMP.

  Po zainstalowaniu Kaspersky Security Center, pliki .mib, potrzebne do zbierania danych statystycznych, zostaną umieszczone w podfolderze SNMP folderu instalacyjnego aplikacji.

Agent sieciowy i Konsola administracyjna nie są wyświetlane na liście modułów. Moduły te są instalowane automatycznie, nie możesz anulować ich instalacji.

W tym kroku musisz określić folder instalacyjny komponentów Serwera administracyjnego. Domyślnie moduły są instalowane w folderze <Dysk>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji. Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

Krok 9. Wybieranie rozmiaru sieci

Określ rozmiar sieci, w której instalowany jest Kaspersky Security Center. W zależności od liczby urządzeń w sieci, kreator odpowiednio konfiguruje instalację i wygląd interfejsu aplikacji.

Poniższa tabela wymienia ustawienia instalacyjne aplikacji i ustawienia wyglądu interfejsu, w zależności od różnych rozmiarów sieci.

Zależność ustawień instalacji od wybranej skali sieci

Ustawienia	1—100 urządzeń	101—1000 urządzeń	1000—5000 urządzeń	Więcej niż 5000 urządzeń
Wyświetlanie w drzewie konsoli węzłów podrzędnych i wirtualnych Serwerów administracyjnych oraz wszystkich ustawień związanych z podrzędnymi i wirtualnymi Serwerami administracyjnymi	Niedostępne	Niedostępne	Dostępne	Dostępne
Wyświetlanie sekcji **Zabezpieczenia** w oknach właściwości Serwera administracyjnego i grup administracyjnych	Niedostępne	Niedostępne	Dostępne	Dostępne
Losowy czas uruchomienia dla zadania aktualizacji na urządzeniach klienckich	Niedostępne	Ponad 5 minut	Ponad 10 minut	Ponad 10 minut

Jeśli łączysz Serwer administracyjny z serwerem bazodanowym MySQL 5.7 lub SQL Express, nie jest zalecane zarządzanie przy pomocy aplikacji liczbą urządzeń większą niż 10 000. W przypadku systemu zarządzania bazą danych MariaDB maksymalna zalecana liczba zarządzanych urządzeń to 20 000.

Krok 10. Wybieranie bazy danych

W tym kroku kreatora wybierz jeden z następujących systemów zarządzania bazami danych (DBMS), który będzie używany do przechowywania bazy danych Serwera administracyjnego:

- **Microsoft SQL Server lub SQL Server Express**
- **MySQL lub MariaDB**
- **PostgreSQL lub Postgres Pro**

Zaleca się zainstalowanie Serwera administracyjnego na serwerze dedykowanym zamiast na kontrolerze domeny. Jeśli instalujesz Kaspersky Security Center na serwerze, który działa jako kontroler domeny tylko do odczytu (RODC), Microsoft SQL Server (SQL Express) nie może zostać zainstalowany lokalnie (na tym samym urządzeniu). W tym przypadku zalecane jest zdalne zainstalowanie Microsoft SQL Server (SQL Express) (na innym urządzeniu) lub tego, którego używasz — MySQL, MariaDB, lub PostgreSQL — jeśli musisz zainstalować system DBMS lokalnie.

Struktura bazy danych Serwera administracyjnego jest opisana w pliku klakdb.chm, umieszczonym w folderze instalacyjnym Kaspersky Security Center. Ten plik jest również dostępny w archiwum w portalu Kaspersky: klakdb.zip.

Krok 11. Konfigurowanie serwera SQL

W tym kroku kreatora określ następujące ustawienia połączenia, w zależności od wybranego systemu zarządzania bazą danych (DBMS):

- Jeśli w poprzednim kroku wybrałeś **Microsoft SQL Server lub SQL Server Express**:

  - W polu **Nazwa instancji serwera SQL** określ nazwę serwera SQL w sieci. Aby wyświetlić listę wszystkich serwerów SQL, które są w sieci, kliknij przycisk **Przeglądaj**. Domyślnie to pole jest puste.

    Jeśli nawiążesz połączenie z serwerem SQL za pośrednictwem portu niestandardowego, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    Nazwa_hosta_serwera_SQL,1433
    ```

    Jeśli chronisz komunikację między Serwerem administracyjnym a serwerem SQL przy pomocy certyfikatu, w polu **Nazwa instancji serwera SQL** określ taką samą nazwę hosta, jaka była użyta w momencie generowania certyfikatu. Jeśli użyjesz nazwanej instancji serwera SQL, wówczas wraz z nazwą hosta serwera SQL określ numer portu oddzielony przecinkiem, na przykład:

    ```
    Nazwa_serwera_SQL,1433
    ```

    Jeśli używasz kilku instancji serwera SQL na tym samym hoście, wówczas dodatkowo określ nazwę instancji oddzieloną lewym ukośnikiem, na przykład:

    ```
    Nazwa_serwera_SQL\Nazwa_instancji_serwera_SQL,1433
    ```

    Jeśli serwer SQL w sieci firmowej ma włączoną funkcję Always On, określ nazwę odbiornika grupy dostępności w polu **Nazwa instancji serwera SQL**. Zauważ, że Serwer administracyjny obsługuje tylko tryb dostępności zatwierdzania synchronicznego, gdy włączona jest funkcja Always On.

  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

  Jeśli chcesz ręcznie zainstalować serwer SQL na urządzeniu, na którym instalujesz Kaspersky Security Center, będziesz musiał zatrzymać instalację i uruchomić ją ponownie po zainstalowaniu serwera SQL. Obsługiwane wersje serwerów SQL są wymienione w wymaganiach systemowych.

  W przypadku, gdy ręcznie instalujesz serwer SQL na zdalnym urządzeniu, nie będzie potrzeby przerywania pracy kreatora instalacji Kaspersky Security Center. Zainstaluj serwer SQL i wznów instalację Kaspersky Security Center.

- Jeśli w poprzednim kroku wybrano **MySQL lub MariaDB**:

  - W polu **Nazwa instancji serwera SQL** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.

  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 3306.

  - W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

- Jeśli w poprzednim kroku wybrano **Postgres**:

  - W polu **Nazwa instancji serwera Postgres** określ nazwę instancji DBMS. Domyślnie, nazwa to adres IP urządzenia, na którym będzie instalowany Kaspersky Security Center.

  - W polu **Port** określ port połączenia Serwera administracyjnego z DBMS. Domyślny numer portu to 5432.

W polu **Nazwa bazy danych** określ nazwę bazy danych, która została utworzona w celu przechowywania danych Serwera administracyjnego. Domyślna wartość to *KAV*.

Krok 12. Wybieranie trybu uwierzytelniania

Określ tryb uwierzytelniania, który będzie używany, gdy Serwer administracyjny połączy się z systemem zarządzania bazami danych (DBMS).

W zależności od wybranego DBMS, możesz wybrać jeden z następujących trybów uwierzytelniania:

- Dla SQL Express lub Microsoft SQL Server wybierz jedną z następujących opcji:

  - **Tryb uwierzytelniania Microsoft Windows**. Weryfikacja uprawnień wykorzystuje konto używane do uruchamiania Serwera administracyjnego.

  - **Tryb uwierzytelniania serwera SQL**. Jeśli wybierzesz tę opcję, do weryfikacji uprawnień zostanie użyte konto określone w oknie. Wypełnij pola **Konto** i **Hasło**.

    Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

  W przypadku obu trybów uwierzytelniania aplikacja sprawdza, czy baza danych jest dostępna. Jeśli baza danych nie jest dostępna, zostanie wyświetlony komunikat o błędzie, a Ty będziesz musiał dostarczyć poprawne dane uwierzytelniające.

  Jeśli baza danych Serwera administracyjnego jest przechowywana na innym urządzeniu, a konto Serwera administracyjnego nie ma uprawnień dostępu do serwera bazy danych, podczas instalowania lub aktualizowania Serwera administracyjnego musisz użyć trybu uwierzytelniania serwera SQL. Może to mieć miejsce, gdy urządzenie przechowujące bazę danych znajduje się poza domeną lub gdy Serwer administracyjny jest instalowany z poziomu konta SystemLokalny.

W przypadku MySQL, MariaDB, PostgreSQL lub Postgres Pro określ konto i hasło.

Krok 13. Wybieranie konta do uruchamiania Serwera administracyjnego

Wybierz konto, z poziomu którego Serwer administracyjny będzie uruchamiany jako usługa.

- **Utwórz konto automatycznie**. Aplikacja tworzy konto pod nazwą KL-AK-*, z którego zostanie uruchomiona usługa kladminserver.

  Możesz wybrać tę opcję, jeśli planujesz umieścić folder współdzielony i DBMS na tym samym urządzeniu co Serwer administracyjny.

- **Wybierz konto**. Usługa Serwera administracyjnego (kladminserver) zostanie uruchomiona z poziomu konta, które wybrałeś.

  Będziesz musiał wybrać konto domenowe, jeśli, na przykład, planujesz używać DBMS jako instancji serwera SQL w dowolnej wersji, w tym SQL Express, który znajduje się na innym urządzeniu, i/lub planujesz umieścić folder współdzielony na innym urządzeniu.

  Kaspersky Security Center obsługuje zarządzane konta usługi (MSA) i grupę zarządzanych kont usługi (gMSA). Jeśli w Twojej domenie używane są tego typu konta, możesz wybrać jedno z nich jako konto dla usługi Serwera administracyjnego.

Przed określeniem MSA lub gMSA musisz zainstalować konto na tym samym urządzeniu, na którym chcesz zainstalować serwer administracyjny. Jeśli konto nie zostało jeszcze zainstalowane, anuluj instalację Serwera administracyjnego, zainstaluj konto, a następnie uruchom ponownie instalację Serwera administracyjnego. Szczegółowe informacje na temat instalacji zarządzanych kont usług na urządzeniu lokalnym można znaleźć w oficjalnej dokumentacji firmy Microsoft.

Aby określić MSA lub gMSA:

1. Kliknij przycisk **Przeglądaj**.
2. W otwartym oknie kliknij przycisk **Typ obiektu**.
3. Wybierz typ **Konto dla usług** i kliknij **OK**.
4. Wybierz odpowiednie konto i kliknij **OK**.

Wybrane konto musi posiadać różne uprawnienia, w zależności od systemu DBMS, którego planujesz używać.

W celach bezpieczeństwa nie należy przydzielać stanu uprzywilejowanego do konta, z poziomu którego uruchamiasz Serwer administracyjny.

Jeżeli w przyszłości będziesz chciał zmienić konto Serwera administracyjnego, będziesz mógł użyć narzędzia do przełączania konta Serwera administracyjnego (klsrvswch).

Krok 14. Wybieranie konta do uruchamiania usług Kaspersky Security Center

Wybierz konto, z poziomu którego usługi Kaspersky Security Center będą uruchomione na tym urządzeniu:

- **Utwórz konto automatycznie**. Kaspersky Security Center tworzy lokalne konto o nazwie KlScSvc na tym urządzeniu w grupie kladmins. Usługi Kaspersky Security Center zostaną uruchomione z poziomu utworzonego konta.
- **Wybierz konto**. Usługi Kaspersky Security Center będą uruchamiane z poziomu wybranego konta.

  Będziesz musiał wybrać konto domenowe, jeśli, na przykład, planujesz zapisywać raporty do folderu znajdującego się na innym urządzeniu lub jeśli jest to wymagane przez politykę bezpieczeństwa organizacji. Konieczne może być także wybranie konta domeny, jeśli instalujesz Serwer administracyjny na klastrze typu failover.

W celach bezpieczeństwa nie należy przydzielać stanu uprzywilejowanego do konta, z poziomu którego uruchamiane są usługi.

Usługa KSN proxy (ksnproxy), usługa Kaspersky activation proxy (klactprx) oraz usługa Kaspersky authentication portal (klwebsrv) będą uruchamiane z poziomu wybranego konta.

Krok 15. Wybieranie folderu współdzielonego

Określ lokalizację i nazwę foldera współdzielonego, który będzie wykorzystywany do następujących zadań:

- Przechowywania plików potrzebnych do przeprowadzenia zdalnej instalacji aplikacji (te pliki są kopiowanie na Serwer administracyjny podczas tworzenia pakietów instalacyjnych).
- Przechowywania uaktualnień pobranych ze źródła uaktualnień na Serwer administracyjny.

Współdzielenie plików (tylko do odczytu) będzie możliwe dla wszystkich użytkowników.

Możesz wybrać jedną z następujących opcji:

- **Utwórz folder współdzielony**. Utwórz nowy folder. W polu do wprowadzenia tekstu określ ścieżkę dostępu do folderu.
- **Wskaż istniejący folder współdzielony**. Wybierz folder współdzielony, który już istnieje.

Folder współdzielony może być folderem lokalnym na urządzeniu, które jest używane do instalacji, lub zdalnym folderem na dowolnym urządzeniu klienckim w obrębie sieci firmowej. Folder współdzielony można wybrać przez kliknięcie przycisku **Przeglądaj** lub ręczne wprowadzenie jego ścieżki w formacie UNC (na przykład \\server\Share) w odpowiednim polu.

Domyślnie instalator tworzy lokalny podfolder Share w folderze aplikacji zawierającym moduły Kaspersky Security Center.

W razie potrzeby folder udostępniony można zdefiniować później.

Krok 16. Konfigurowanie połączenia z Serwerem administracyjnym

Skonfiguruj połączenie z Serwerem administracyjnym:

- **Port**

  Numer portu używanego do nawiązywania połączenia z Serwerem administracyjnym.

  Domyślny numer portu to 14000.

- **Port SSL**

  Numer portu Secure Sockets Layer (SSL) używanego do nawiązywania bezpiecznego połączenia z Serwerem administracyjnym poprzez SSL.

  Domyślny numer portu to 13000.

- **Długość klucza szyfrowania**

  Wybierz długość klucza szyfrowania: 1024 bity lub 2048 bitów.

  Klucz szyfrowania o długości 1024 bitów w mniejszym stopniu obciąża procesor, ale jest uznawany za przestarzały, ponieważ nie zapewnia niezawodnego szyfrowania ze względu na swoją specyfikację techniczną. Dodatkowo, istniejący sprzęt okaże się niekompatybilny z certyfikatami SSL zawierającymi 1024-bitowe klucze.

  Klucz szyfrowania o długości 2048 bitów spełnia wszystkie najnowocześniejsze standardy szyfrowania. Jednakże użycie 2048-bitowego klucza szyfrowania może zwiększyć obciążenie procesora.

  Domyślnie wybrana jest opcja **2048 bitów (największe bezpieczeństwo)**.

Jeżeli Serwer administracyjny jest zainstalowany na urządzeniu działającym pod kontrolą systemu Microsoft Windows XP Service Pack 2, wówczas wbudowana zapora sieciowa będzie blokowała porty TCP: 13000 i 14000. Dlatego też, aby zezwolić na dostęp do Serwera administracyjnego na urządzeniu po instalacji, należy ręcznie otworzyć te porty.

Krok 17. Określanie adresu Serwera administracyjnego

Określ adres Serwera administracyjnego. Możesz wybrać jedną z następujących opcji:

- **Nazwa domeny DNS**. Metoda ta jest użyteczna, gdy sieć zawiera serwer DNS, którego urządzenia klienckie mogą użyć do uzyskania adresu Serwera administracyjnego.
- **Nazwa NetBIOS**. Metoda ta jest przydatna, gdy urządzenia klienckie uzyskują adres Serwera administracyjnego za pośrednictwem protokołu NetBIOS lub gdy w sieci dostępny jest serwer WINS.
- **Adres IP**. Metoda ta jest używana, gdy Serwer administracyjny posiada stały adres IP, który w przyszłości nie zostanie zmieniony.

Krok 18. Adres Serwera administracyjnego dla podłączenia urządzeń mobilnych

Ten krok kreatora instalacji jest dostępny, jeśli moduł Zarządzanie urządzeniami mobilnymi został wybrany do zainstalowania.

W oknie **Adres do podłączenia urządzeń mobilnych** określ zewnętrzny adres Serwera administracyjnego dla podłączenia urządzeń mobilnych, które znajdują się poza siecią lokalną. Możesz określić adres IP lub system nazw domen (DNS) Serwera administracyjnego.

Krok 19. Wypakowywanie i instalowanie plików na dysku twardym

Po skonfigurowaniu instalacji modułów Kaspersky Security Center, możesz rozpocząć instalację plików na dysku twardym.

Jeśli instalacja wymaga dodatkowych programów, kreator instalacji powiadomi Cię o tym w oknie **Instalacja wymaganego oprogramowania** przed rozpoczęciem instalacji Kaspersky Security Center. Wymagane programy są instalowane automatycznie po kliknięciu przycisku **Dalej**.

W ostatnim kroku możesz wybrać, którą konsolę uruchomić do pracy z Kaspersky Security Center:

- **Uruchom Konsolę administracyjną MMC**
- **Uruchom Kaspersky Security Center Web Console**

  Ta opcja jest dostępna tylko wtedy, gdy w jednym z poprzednich kroków wybrano instalację Kaspersky Security Center Web Console.

Możesz także kliknąć **Zakończ**, aby zamknąć kreator bez rozpoczynania pracy z Kaspersky Security Center. Możesz rozpocząć pracę później w dowolnym momencie.

Przy pierwszym uruchomieniu Konsoli administracyjnej lub Kaspersky Security Center Web Console możesz przeprowadzić wstępną konfigurację aplikacji.

Instalowanie Serwera administracyjnego w trybie nieinteraktywnym

Serwer administracyjny może zostać zainstalowany w trybie nieinteraktywnym, czyli bez interaktywnego wprowadzania ustawień instalacji.

W celu zainstalowania Serwera administracyjnego na urządzeniu lokalnym w trybie nieinteraktywnym:

1. Przeczytaj Umowę licencyjną. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej.

2. Przeczytaj Politykę prywatności. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i zgadzasz się, żeby Twoje dane były zarządzane i przesyłane (w tym do innych krajów) w sposób opisany w Polityce prywatności.

3. Uruchom polecenie

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1
<parametry_instalacji>"
```

gdzie `setup_parameters` to lista parametrów i ich odpowiednich wartości oddzielonych spacjami (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). Plik setup.exe znajduje się w folderze Server, który jest częścią pakietu dystrybucyjnego Kaspersky Security Center.

Nazwy i możliwe wartości parametrów, które mogą być używane podczas instalacji Serwera administracyjnego w trybie nieinteraktywnym, znajdują się w tabeli poniżej.

Parametry instalacji Serwera administracyjnego w trybie nieinteraktywnym

Nazwa parametru	Opis parametru	Dostępne wartości
EULA	Akceptacja postanowień i warunków Umowy licencyjnej.	• 1—W pełni przeczytałem, rozumiem i akceptuję warunki Umowy licencyjnej. • Inna wartość lub bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
PRIVACYPOLICY	Akceptacja postanowień i warunków Polityki prywatności.	• 1—Jestem świadomy i wyrażam zgodę na przetwarzanie oraz przesyłanie moich danych (również do innych krajów) zgodnie z Polityką prywatności. Potwierdzam, że w pełni przeczytałem i rozumiem Politykę prywatności.

		• Inna wartość lub bez wartości —Nie akceptuję postanowień i warunków Polityki prywatności (instalacja nie zostanie wykonana).
INSTALLATIONMODETYPE	Typ instalacji Serwera administracyjnego.	• Standard—instalacja standardowa. • Custom—instalacja niestandardowa.
INSTALLDIR	Ścieżka do folderu instalacyjnego Serwera administracyjnego.	Wartość wiersza.
ADDLOCAL	Lista instalowanych komponentów Serwera administracyjnego (oddzielone przecinkami).	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimalna lista komponentów wystarczających do poprawnego zainstalowania Serwera administracyjnego: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.`
NETRANGETYPE	Rozmiar sieci (liczba urządzeń w sieci).	• NRT_1_100 — od 1 do 100 urządzeń. • NRT_100_1000 – od 101 do 1 000 urządzeń. • NRT_GREATER_1000—więcej niż 1 000 urządzeń.
SRV_ACCOUNT_TYPE	Tryb określania konta, z poziomu którego Serwer administracyjny zostanie uruchomiony jako usługa.	• SrvAccountDefault —konto jest tworzone automatycznie. • SrvAccountUser —konto jest określane ręcznie. W tym przypadku należy określić wartości dla parametrów `SERVERACCOUNTNAME` i `SERVERACCOUNTPWD`.
SERVERACCOUNTNAME	Nazwa konta, z poziomu którego Serwer administracyjny zostanie uruchomiony jako usługa. Należy określić wartość dla ustawienia, jeśli istnieje SRV_ACCOUNT_TYPE=SrvAccountUser.	Wartość wiersza.

SERVERACCOUNTPWD	Hasło do konta, z poziomu którego Serwer administracyjny będzie uruchamiany jako usługa. Należy określić wartość dla ustawienia, jeśli istnieje SRV_ACCOUNT_TYPE=SrvAccountUser.	Wartość wiersza.
SERVERCER	Długość klucza certyfikatu Serwera administracyjnego (bity).	• 1 — długość klucza certyfikatu Serwera administracyjnego wynosi 2048 bity. • Bez wartości —długość klucza certyfikatu Serwera administracyjnego wynosi 1 024 bity.
DBTYPE	Typ bazy danych, która będzie używana do przechowywania bazy danych Serwera administracyjnego. Ten parametr jest obowiązkowy.	• MySQL—używana będzie baza danych MySQL lub MariaDB. W tym przypadku należy określić wartości parametrów `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME`, oraz `MYSQLACCOUNTPWD`. • MSSQL—używana będzie baza danych Microsoft SQL Server (SQL Express). W tym przypadku należy określić wartości dla parametrów `MSSQLSERVERNAME`, `MSSQLDBNAME` i `MSSQLAUTHTYPE`. • POSTGRES — zostanie użyta baza danych PostgreSQL lub Postgres Pro. W takim przypadku należy określić wartości parametrów `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` oraz `POSTGRESACCOUNTPWD`.
MYSQLSERVERNAME	Pełna nazwa serwera SQL. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	Wartość wiersza.
MYSQLSERVERPORT	Numer portu do nawiązania połączenia z serwerem SQL. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	Wartość numeryczna.
MYSQLDBNAME	Nazwa bazy danych, która zostanie utworzona w celu przechowywania danych Serwera administracyjnego.	Wartość wiersza.

	Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	
MYSQLACCOUNTNAME	Nazwa konta do łączenia z bazą danych. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	Wartość wiersza.
MYSQLACCOUNTPWD	Hasło do konta do łączenia z bazą danych. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MySQL.	Wartość wiersza.
MSSQLSERVERNAME	Pełna nazwa serwera SQL. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MSSQL.	Wartość wiersza.
MSSQLDBNAME	Nazwa bazy danych. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MSSQL.	Wartość wiersza.
MSSQLAUTHTYPE	Typ uwierzytelniania podczas nawiązywania połączenia z serwerem SQL. Należy określić wartość dla parametru, jeśli istnieje DBTYPE=MSSQL.	• Windows—tryb uwierzytelniania Microsoft Windows. • SQLServer—tryb uwierzytelniania serwera SQL. W tym przypadku należy określić wartości dla parametrów `MSSQLACCOUNTNAME` i `MSSQLACCOUNTPWD`.
MSSQLACCOUNTNAME	Nazwa konta do nawiązania połączenia z serwerem SQL. Należy określić wartość dla parametru, jeśli istnieje MSSQLAUTHTYPE=SQLServer.	Wartość wiersza.
MSSQLACCOUNTPWD	Hasło do konta do nawiązania połączenia z serwerem SQL. Należy określić wartość dla parametru, jeśli istnieje MSSQLAUTHTYPE=SQLServer.	Wartość wiersza.
CREATE_SHARE_TYPE	Metoda określania folderu współdzielonego.	• Create—tworzy nowy folder współdzielony. W tym przypadku należy określić wartości dla parametrów `SHARELOCALPATH` i `SHAREFOLDERNAME`. • ChooseExisting—wybiera istniejący folder. W tym przypadku należy określić wartość dla parametru `EXISTSHAREFOLDERNAME`.
SHARELOCALPATH	Pełna ścieżka dostępu do folderu lokalnego. Należy określić wartość dla parametru, jeśli istnieje CREATE_SHARE_TYPE=Create	Wartość wiersza.

SHAREFOLDERNAME	Nazwa sieciowa folderu współdzielonego. Należy określić wartość dla parametru, jeśli istnieje CREATE_SHARE_TYPE=Create.	Wartość wiersza.
EXISTSHAREFOLDERNAME	Pełna ścieżka dostępu do istniejącego folderu współdzielonego. Należy określić wartość dla parametru, jeśli istnieje CREATE_SHARE_TYPE=ChooseExisting.	Wartość wiersza.
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym.	Wartość numeryczna.
SERVERSSLPORT	Numer portu dla szyfrowanego połączenia z Serwerem administracyjnym przy użyciu protokołu SSL.	Wartość numeryczna.
SERVERADDRESS	Adres Serwera administracyjnego.	Wartość wiersza.
MOBILESERVERADDRESS	Adres Serwera administracyjnego dla podłączenia urządzeń mobilnych.	Wartość wiersza.

Szczegółowy opis parametrów instalacji Serwera administracyjnego znajduje się w sekcji Instalacja niestandardowa.

Instalowanie Konsoli administracyjnej na stacji roboczej administratora

Możesz oddzielnie zainstalować Konsolę administracyjną na stacji roboczej administratora i zarządzać Serwerem administracyjnym przez sieć przy pomocy tej Konsoli.

W celu zainstalowania Konsoli administracyjnej na stacji roboczej administratora:

1. Uruchom plik wykonywalny setup.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky do zainstalowania.

2. W oknie wyboru aplikacji kliknij odnośnik **Zainstaluj wyłącznie Konsolę administracyjną Kaspersky Security Center**, aby uruchomić kreator instalacji Konsoli administracyjnej. Postępuj zgodnie z instrukcjami kreatora.

3. Wybierz folder docelowy. Domyślnie jest to <Dysk>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji. Można zmienić folder docelowy przy użyciu przycisku **Przeglądaj**.

4. W ostatnim oknie kreatora instalacji kliknij przycisk **Uruchom**, aby uruchomić instalację Konsoli administracyjnej.

Po zakończeniu pracy kreatora, Konsola administracyjna zostanie zainstalowana na stacji roboczej administratora.

W celu zainstalowania Konsoli administracyjnej na stacji roboczej administratora w trybie nieinteraktywnym:

1. Przeczytaj Umowę licencyjną. Użyj poniższego polecenia tylko wtedy, gdy rozumiesz i akceptujesz warunki Umowy licencyjnej.

2. W folderze `Distrib\Console` zestawu dystrybucyjnego Kaspersky Security Center uruchom plik setup.exe za pomocą następującego polecenia:

```
setup.exe /s /v"EULA=1"
```

Jeśli chcesz zainstalować wszystkie wtyczki zarządzające z folderu `Distrib\Console\Plugins` wraz z Konsolą administracyjną, uruchom następujące polecenie:

```
setup.exe /s /v"EULA=1" /pALL
```

Jeśli chcesz określić, które wtyczki zarządzające mają zostać zainstalowane z folderu `Distrib\Console\Plugins` wraz z Konsolą administracyjną, określ wtyczki po przełączniku „/p" i oddziel je średnikiem:

```
setup.exe /s /v"EULA=1" /pP1;P2;P3
```

gdzie `P1`, `P2`, `P3` to nazwy wtyczek, które odpowiadają nazwom folderów wtyczek w folderze `Distrib\Console\Plugins`. Na przykład:

```
setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
```

Konsola administracyjna i wtyczki zarządzające (jeśli istnieją) zostaną zainstalowane na stacji roboczej administratora.

Po zainstalowaniu Konsoli administracyjnej musisz połączyć się z Serwerem administracyjnym. W tym celu uruchom Konsolę administracyjną i w otwartym oknie określ nazwę lub adres IP urządzenia, na którym został zainstalowany Serwer administracyjny, a także ustawienia konta używanego do nawiązywania połączenia. Po nawiązaniu połączenia z Serwerem administracyjnym możesz zarządzać systemem ochrony antywirusowej przy pomocy Konsoli administracyjnej.

Możesz usunąć Konsolę administracyjną przy pomocy standardowych narzędzi dodawania/usuwania z Microsoft Windows.

Zmiany w systemie po instalacji Kaspersky Security Center

Ikona Konsoli administracyjnej

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

Usługi Serwera administracyjnego i Agenta sieciowego

Serwer administracyjny i Agent sieciowy zostaną zainstalowane na urządzeniu jako usługi z właściwościami wymienionymi poniżej. Tabela zawiera również atrybuty innych usług, które są stosowane na urządzeniu po zainstalowaniu Serwera administracyjnego.

Właściwości usług Kaspersky Security Center

Moduł	Nazwa usługi	Wyświetlona nazwa usługi	Konto
Serwer administracyjny	kladminserver	Serwer administracyjny Kaspersky Security Center	Nieuprzywilejowane konto dedykowane lub zdefiniowane przez użytkownika w formacie KL-AK-*, utworzone podczas instalacji
Agent sieciowy	klnagent	Agent sieciowy	System lokalny

		Kaspersky Security Center	
Serwer sieciowy umożliwiający dostęp do konsoli Kaspersky Security Center Web Console i zarządzanie siecią wewnętrzną organizacji	klwebsrv	Serwer sieciowy Kaspersky	Dedykowane konto bez uprawnień KlScSvc
Aktywacja serwera proxy	klactprx	Kaspersky activation proxy server	Dedykowane konto bez uprawnień KlScSvc
Serwer KSN proxy	ksnproxy	Serwer proxy Kaspersky Security Network	Dedykowane konto bez uprawnień KlScSvc

Usługi Kaspersky Security Center Web Console

Jeśli zainstalujesz Kaspersky Security Center Web Console na urządzeniu, zostaną wdrożone następujące usługi (zobacz poniższą tabelę):

Usługi Kaspersky Security Center Web Console

Wyświetlona nazwa usługi	Konto
Kaspersky Security Center Service Web Console	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web Console	Usługa sieciowa
Kaspersky Security Center Product Plugins Server	NT Service/KSCWebConsolePlugin
Usługa zarządzania Kaspersky Security Center Web Console	System lokalny
Kolejka wiadomości Kaspersky Security Center Web Console	NT Service/KSCWebConsoleMessageQueue

Wersja serwerowa Agenta sieciowego

Wersja serwerowa Agenta sieciowego zostanie zainstalowana na urządzeniu wraz z Serwerem administracyjnym. Wersja serwerowa Agenta sieciowego jest częścią Serwera administracyjnego i jest instalowana i usuwana wraz z Serwerem administracyjnym. Może ona współdziałać z lokalnie zainstalowanym Serwerem administracyjnym. Nie ma konieczności konfigurowania ustawień połączenia Agenta sieciowego z Serwerem administracyjnym: ustawienia te są implementowane poprzez funkcje programu, ponieważ składniki są instalowane na tym samym urządzeniu. Wersja serwerowa Agenta sieciowego jest instalowana z tymi samymi właściwościami co standardowa wersja Agenta i realizuje te same funkcje zarządzania aplikacją. Ta wersja będzie zarządzana przez zasadę grupy administracyjnej, do której należy urządzenie klienckie Serwera administracyjnego. Dla wersji serwerowej Agenta sieciowego wszystkie zadania są tworzone ze zbioru tych przeznaczonych dla Serwera administracyjnego, za wyjątkiem zadania zmiany Serwera.

Agent sieciowy nie może zostać zainstalowany oddzielnie na urządzeniu, na którym jest już zainstalowany Serwer administracyjny.

Możesz wyświetlić właściwości każdej usługi Serwera administracyjnego i Agenta sieciowego, jak również monitorować ich działanie przy pomocy standardowych narzędzi zarządzających Microsoft Windows: Zarządzanie komputerem\Usługi. Informacja o aktywności usługi Serwera administracyjnego Kaspersky jest przechowywana w dzienniku systemu Microsoft Windows, w oddzielnej gałęzi dziennika zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany Serwer administracyjny.

Zalecamy unikanie ręcznego uruchamiania i zatrzymywania usług oraz pozostawiania niezmienionych kont usług w ustawieniach usług. Jeśli to konieczne, możesz zmodyfikować konto usługi Serwera administracyjnego przy użyciu narzędzia klsrvswch.

Konta użytkowników i grupy użytkowników

Instalator Serwera administracyjnego domyślnie tworzy następujące konta:

- KL-AK-*: konto usługi Serwera administracyjnego
- KlScSvc: konto dla innych usług z puli Serwera administracyjnego
- KlPxeUser: konto do zdalnej instalacji systemów operacyjnych

Jeśli podczas działania instalatora wybrałeś inne konta dla usługi Serwera administracyjnego i innych usług, używane są określone konta.

Na urządzeniu z zainstalowanym Serwerem administracyjnym zostaną także automatycznie utworzone lokalne grupy zabezpieczeń o nazwach KLAdmins i KLOperators z ich odpowiednimi zestawami uprawnień.

Nie zaleca się instalacji Serwera administracyjnego na kontrolerze domeny; jeśli jednak instalujesz Serwer administracyjny na kontrolerze domeny, należy uruchomić instalator z uprawnieniami administratora. W tym przypadku instalator automatycznie tworzy grupy bezpieczeństwa domeny o nazwie KLAdmins i KLOperators. Jeśli instalujesz Serwer administracyjne na komputerze, który nie znajduje się w kontrolerze domeny, powinieneś uruchomić instalator z uprawnieniami administratora lokalnego. W tym przypadku instalator automatycznie tworzy lokalne grupy bezpieczeństwa o nazwie KLAdmins i KLOperators.

Podczas konfigurowania powiadamiania pocztą elektroniczną, konieczne może być utworzenie konta na serwerze pocztowym dla autoryzacji ESMTP.

Dezinstalowanie aplikacji

Możesz usunąć Kaspersky Security Center przy pomocy standardowych narzędzi dodawania/usuwania Microsoft Windows. Usuwanie aplikacji wymaga uruchomienia kreatora, który usunie wszystkie moduły aplikacji z urządzenia (łącznie z wtyczkami). Kreator sprawia, że domyślna przeglądarka otwiera stronę internetową z ankietą, na której możesz nam powiedzieć, dlaczego zdecydowałeś się zaprzestać korzystania z Kaspersky Security Center. Jeśli podczas działania kreatora nie wybrałeś do usunięcia folderu współdzielonego (Share), usuń go ręcznie po zakończeniu wszystkich zadań, które mają do niego dostęp.

Po usunięciu aplikacji, niektóre jej pliki mogą pozostać w folderze tymczasowym systemu.

Kreator tworzenia zadania usuwania aplikacji zasugeruje przechowywanie kopii zapasowej Serwera administracyjnego.

Gdy aplikacja zostanie usunięta z systemów Microsoft Windows 7 i Microsoft Windows 2008, może nastąpić przedwczesne zakończenie działania kreatora tworzenia zadania usuwania aplikacji. Można tego uniknąć przez wyłączenie w systemie operacyjnym Kontroli konta użytkownika (UAC) i ponowne uruchomienie usuwania aplikacji.

Informacje o aktualizacji Kaspersky Security Center

Ta sekcja zawiera informacje o tym, jak zaktualizować Kaspersky Security Center z poprzedniej wersji. Możesz zaktualizować Kaspersky Security Center na różne sposoby, w zależności od tego, czy Kaspersky Security Center został zainstalowany lokalnie, czy na węzłach klastra typu failover Kaspersky.

Podczas aktualizacji równoczesne korzystanie z DBMS przez Serwer administracyjny i inną aplikację jest surowo zabronione.

Podczas, gdy aktualizujesz Kaspersky Security Center z poprzedniej wersji, wszystkie zainstalowane wtyczki obsługiwanych aplikacji Kaspersky są zachowywane. Wtyczka Serwera administracyjnego oraz wtyczka Agenta sieciowego są aktualizowane automatycznie (zarówno dla Konsoli administracyjnej, jak i dla Kaspersky Security Center Web Console).

Scenariusz: Aktualizowanie Kaspersky Security Center i zarządzanych aplikacji zabezpieczających

Ta sekcja opisuje główny krótki scenariusz aktualizacji Kaspersky Security Center i zarządzanych aplikacji zabezpieczających.

Aktualizacja Kaspersky Security Center i zarządzanych aplikacji zabezpieczających odbywa się w etapach:

1. **Sprawdzanie wymagań sprzętowych i programowych**

   Upewnij się, że sprzęt spełnia wymagania i zainstaluj wymagane aktualizacje.

2. **Rozplanowywanie zasobów**

   Oceń, ile miejsca na dysku zajmuje Twoja baza danych. Upewnij się, że posiadasz wystarczającą ilość miejsca na dysku do przechowywania kopii zapasowej ustawień i bazy danych Serwera administracyjnego.

3. **Uzyskiwanie pliku instalatora dla Kaspersky Security Center**

   Uzyskiwanie pliku wykonywalnego dla bieżącej wersji Kaspersky Security Center i zapisywanie go na urządzeniu, które działa jako Serwer administracyjny. Zapoznaj się z Informacjami o kompilacji dla nowej wersji Kaspersky Security Center, której chcesz użyć.

4. **Tworzenie kopii zapasowej poprzedniej wersji**

   Użyj narzędzia do tworzenia kopii zapasowej i odzyskiwania danych, aby utworzyć kopię zapasową danych Serwera administracyjnego. Możesz także utworzyć zadanie tworzenia kopii zapasowej.

   Zaleca się wyeksportowanie listy zainstalowanych wtyczek.

5. **Uruchamianie instalatora**

   Uruchom plik wykonywalny dla najnowszej wersji Kaspersky Security Center. Podczas uruchamiania pliku określ, czy masz kopię zapasową i określ jej lokalizację. Twoje dane zostaną przywrócone z kopii zapasowej.

6. **Aktualizowanie zarządzanych aplikacji**

   Możesz zaktualizować aplikację, jeśli jest dostępna nowsza wersja. Zapoznaj się z listą obsługiwanych aplikacji Kaspersky i upewnij się, że Twoja wersja Kaspersky Security Center jest kompatybilna z tą aplikacją. Następnie przeprowadź aktualizację aplikacji w sposób opisany w jej Informacjach o kompilacji.

Wyniki

Po zakończeniu scenariusza aktualizacji, upewnij się, że nowa wersja Serwera administracyjnego została pomyślnie zainstalowana w konsoli Microsoft Management Console. Kliknij **Pomoc → Informacje o Kaspersky Security Center**. Zostanie wyświetlona wersja.

Aby upewnić się, że korzystasz z nowszej wersji Serwera administracyjnego w Kaspersky Security Center Web Console, w górnej części ekranu kliknij ikonę ustawienia ( ) obok nazwy Serwera administracyjnego. W otwartym oknie właściwości Serwera administracyjnego, na zakładce **Ogólne** wybierz sekcję **Ogólne**. Zostanie wyświetlona wersja.

Jeśli chcesz odzyskać dane Serwera administracyjnego, wykonaj czynności opisane w następującym temacie: Tworzenie kopii zapasowej i przywracanie danych w trybie interaktywnym.

Jeśli zaktualizowałeś zarządzaną aplikację zabezpieczającą, upewnij się, że jest ona poprawnie zainstalowana na zarządzanym urządzeniu (zarządzanych urządzeniach). Więcej informacji znajdziesz w dokumentacji dla tej aplikacji.

Aktualizowanie Kaspersky Security Center z poprzedniej wersji

Następujący temat opisuje zalecane kroki przygotowania do uaktualnienia: Aktualizowanie Kaspersky Security Center i zarządzanych aplikacji zabezpieczających.

Możesz zainstalować Serwer administracyjny w wersji 14.2 na urządzeniu, na którym jest zainstalowana wcześniejsza wersja Serwera administracyjnego (począwszy od wersji 11 (11.0.0.1131b)). Podczas aktualizowania do wersji 14.2 wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

Jeżeli podczas instalacji Serwera administracyjnego pojawią się problemy, będziesz mógł przywrócić poprzednią wersję Serwera administracyjnego przy pomocy kopii zapasowej danych Serwera administracyjnego utworzonej przed aktualizacją.

Jeśli w sieci zainstalowano przynajmniej jeden Serwer administracyjny w nowej wersji, inne Serwery administracyjne w sieci mogą zostać zaktualizowane przy pomocy zadania zdalnej instalacji, które korzysta z pakietu instalacyjnego Serwera administracyjnego.

Jeśli wdrożyłeś klaster typu failover Kaspersky, możesz również zaktualizować Kaspersky Security Center na jego węzłach.

W celu zaktualizowania wcześniejszej wersji Serwera administracyjnego do wersji 14.2:

1. Uruchom plik ksc_14.2_<build number>_full_<language>.exe dla wersji 14.2 (możesz pobrać ten plik ze strony internetowej Kaspersky).

2. W oknie, które zostanie otwarte, kliknij odnośnik **Zainstaluj Kaspersky Security Center 14.2**, aby uruchomić Kreatora instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

3. Przeczytaj treść Umowy licencyjnej i Polityki prywatności. Jeśli zgadzasz się na wszystkie warunki Umowy licencyjnej i Polityki prywatności, w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących:** zaznacz następujące pola:

   - **Warunki i postanowienia tej Umowy licencyjnej**
   - **Politykę prywatności opisującą zasady przetwarzania danych**

   Instalacja aplikacji na urządzeniu będzie kontynuowana po zaznaczeniu pól. Kreator instalacji wyświetla pytanie o utworzenie kopii zapasowej danych Serwera administracyjnego dla wcześniejszej wersji.

   Kaspersky Security Center obsługuje odzyskiwanie danych z kopii zapasowej utworzonej za pomocą starszej wersji Serwera administracyjnego.

4. Jeżeli chcesz utworzyć kopię zapasową danych Serwera administracyjnego, określ to w otwartym oknie **Kopia zapasowa Serwera administracyjnego**.

   Kopia zapasowa jest tworzona przez narzędzie klbackup. Narzędzie to jest zawarte w pakiecie dystrybucyjnym aplikacji i znajduje się w głównym folderze instalacyjnym Kaspersky Security Center.

5. Zainstaluj Serwer administracyjny w wersji 14.2, postępując zgodnie z instrukcjami Kreatora instalacji.

   Jeśli pojawi się wiadomość, że usługa Kaspersky Security Center Web Console jest zajęta, w oknie kreatora kliknij przycisk **Ignore**.

   > Należy unikać przerywania działania kreatora instalacji. W przypadku anulowania aktualizacji na etapie instalacji Serwera administracyjnego może spowodować błąd zaktualizowanej wersji Kaspersky Security Center.

6. Dla urządzeń, na których jest instalowana wcześniejsza wersja Agenta sieciowego, utwórz i uruchom zadanie zdalnej instalacji nowej wersji Agenta sieciowego.

   > Zalecamy aktualizację Agenta sieciowego dla systemu Linux do tej samej wersji co Kaspersky Security Center.

   Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

Aktualizowanie Kaspersky Security Center na węzłach klastra trybu failover Kaspersky

Możesz zainstalować Serwer administracyjny w wersji 14.2 na każdym węźle klastra pracy awaryjnej Kaspersky, na którym jest zainstalowana wcześniejsza wersja Serwera administracyjnego (począwszy od wersji 13.2). Podczas aktualizowania do wersji 14.2 wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

> Jeśli wcześniej zainstalowałeś Kaspersky Security Center na urządzeniach lokalnie, możesz również zaktualizować Kaspersky Security Center na tych urządzeniach.

Instalowanie Kaspersky Security Center na węzłach klastra trybu failover Kaspersky:

1. Wykonaj następujące czynności na aktywnym węźle klastra:

   a. Uruchom plik wykonywalny ksc_14.2_<numer kompilacji>_full_<wersja językowa>.exe.

   Zostanie otwarte okno z pytaniem o wybranie aplikacji firmy Kaspersky w celu aktualizacji. Kliknij odnośnik **Zainstaluj Serwer administracyjny Kaspersky Security Center** uruchomić Kreator instalacji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

   b. Przeczytaj treść Umowy licencyjnej i Polityki prywatności. Jeśli zgadzasz się na wszystkie warunki Umowy licencyjnej i Polityki prywatności, w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących:** zaznacz następujące pola:

   - **Warunki i postanowienia tej Umowy licencyjnej**
   - **Politykę prywatności opisującą zasady przetwarzania danych**

   Zaznacz oba pola wyboru, aby kontynuować instalację.

   Jeśli nie akceptujesz Umowy licencyjnej lub Polityki prywatności, kliknij przycisk **Anuluj**, aby anulować aktualizację.

   c. W oknie **Typ instalacji na klastrze**, dla którego chcesz zaktualizować Kaspersky Security Center.

   Następnie instalator konfiguruje i kończy aktualizację Serwera administracyjnego. Podczas aktualizacji nie można zmienić ustawień Serwera administracyjnego.

2. Wykonaj te same czynności na węźle pasywnym klastra pracy awaryjnej Kaspersky, co na węźle aktywnym. W przypadku wybrania opcji **Klaster trybu failover firmy Microsoft (instalacja na wszystkich węzłach klastra)** w oknie **Typ instalacji na klastrze** pomiń ten krok.

3. Uruchom klaster.

W rezultacie zainstalowano Serwer administracyjny najnowszej wersji na węzłach klastra typu failover Kaspersky.

Wstępna konfiguracja Kaspersky Security Center

Ta sekcja opisuje kroki, jakie musisz podjąć po zainstalowaniu Kaspersky Security Center, aby przeprowadzić jego wstępną konfigurację.

Przewodnik zwiększania bezpieczeństwa

Przewodnik zwiększania bezpieczeństwa jest przeznaczony dla profesjonalistów, którzy instalują i administrują Kaspersky Security Center, a także dla tych, którzy zapewniają wsparcie techniczne organizacjom korzystającym z Kaspersky Security Center.

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

Przewodnik zwiększania bezpieczeństwa zawiera następujące informacje:

- Wybór architektury Serwera administracyjnego

- Konfigurowanie bezpiecznego połączenia z Serwerem administracyjnym
- Konfigurowanie kont w celu uzyskania dostępu do Serwera administracyjnego
- Zarządzanie ochroną Serwera administracyjnego i urządzeń klienckich
- Konfigurowanie ochrony dla zarządzanych aplikacji
- Konserwacja Serwera administracyjnego
- Przesyłanie informacji do aplikacji firm trzecich

Przed rozpoczęciem pracy z Serwerem administracyjnym Kaspersky Security Center wyświetli monit o przeczytanie skróconej wersji Przewodnika zwiększania bezpieczeństwa.

Pamiętaj, że nie możesz korzystać z Serwera administracyjnego, dopóki nie potwierdzisz przeczytania Przewodnika zwiększania bezpieczeństwa.

Aby przeczytać Przewodnik zwiększania bezpieczeństwa:

1. Otwórz Konsolę administracyjną lub Kaspersky Security Center Web Console i zaloguj się do konsoli. Konsola sprawdza potwierdzenie przeczytania aktualnej wersji Przewodnika zwiększania bezpieczeństwa.

   Jeśli jeszcze nie znasz treści Przewodnika zwiększania bezpieczeństwa, otworzy się okno i wyświetli jego krótką wersję.

2. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz wyświetlić skróconą wersję Przewodnika zwiększania bezpieczeństwa w formie dokumentu tekstowego, kliknij łącze **Otwórz w nowym oknie**.
   - Jeśli chcesz zobaczyć pełną wersję Przewodnika zwiększania bezpieczeństwa, kliknij łącze **Otwórz Przewodnik zwiększania bezpieczeństwa w Pomocy online**.

3. Po przeczytaniu Przewodnika zwiększania bezpieczeństwa zaznacz pole **wyboru Potwierdzam, przeczytanie w całości i zrozumienie Przewodnika zwiększania bezpieczeństwa**, a następnie kliknij przycisk **Akceptuj**.

Teraz możesz pracować z Serwerem administracyjnym.

Gdy pojawi się nowa wersja Przewodnika zwiększania bezpieczeństwa, Kaspersky Security Center wyświetli monit o jej przeczytanie.

Kreator wstępnej konfiguracji Serwera administracyjnego

Ta sekcja zawiera informacje o działaniu kreatora wstępnej konfiguracji Serwera administracyjnego.

Informacje o kreatorze wstępnej konfiguracji

Ta sekcja zawiera informacje o działaniu kreatora wstępnej konfiguracji Serwera administracyjnego.

Kreator wstępnej konfiguracji Serwera administracyjnego umożliwia utworzenie minimalnej ilości potrzebnych zadań i zasad, dostosowanie minimalnych ustawień, pobranie i zainstalowanie wtyczek dla zarządzanych aplikacji firmy Kaspersky, a także utworzenie pakietów instalacyjnych zarządzanych aplikacji firmy Kaspersky. Przy pierwszym uruchomieniu kreatora możesz wprowadzić w aplikacji następujące zmiany:

- Pobierz i zainstaluj wtyczki dla zarządzanych aplikacji. Po zakończeniu pracy kreatora wstępnej konfiguracji, lista zainstalowanych wtyczek zarządzających zostanie wyświetlona w sekcji **Zaawansowane → Szczegóły zainstalowanych wtyczek administrujących aplikacją** okna właściwości Serwera administracyjnego.

- Utwórz pakiety instalacyjne zarządzanych aplikacji firmy Kaspersky. Po zakończeniu pracy Kreatora wstępnej konfiguracji, pakiety instalacyjne Agenta sieciowego dla systemu for Windows i zarządzanych aplikacji firmy Kaspersky są wyświetlane na liście **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

- Dodaj pliki klucza lub wprowadź kody aktywacyjne, które mogą być automatycznie przesyłane do urządzeń w grupach administracyjnych. Po zakończeniu pracy Kreatora wstępnej konfiguracji, informacje o kluczach licencyjnych są wyświetlane na liście **Serwer administracyjny → Licencje Kaspersky** oraz w sekcji **Klucze licencyjne** okna właściwości Serwera administracyjnego.

- Skonfigurować interakcję z Kaspersky Security Network (KSN).

- Skonfigurować dostarczanie powiadomień informujących o zdarzeniach występujących podczas działania Serwera administracyjnego i zarządzanych aplikacji (w celu zapewnienia poprawnego działania opcji dostarczania powiadomień, na Serwerze administracyjnym i wszystkich urządzeniach, na które mają być wysyłane powiadomienia, powinna być włączona usługa Posłaniec). Po zakończeniu pracy kreatora wstępnej konfiguracji, ustawienia powiadomień e-mail są wyświetlane w sekcji **Powiadamianie** okna właściwości Serwera administracyjnego.

- Dostosować ustawienia aktualizacji oraz ustawienia eliminowania luk dla aplikacji zainstalowanych na urządzeniach.

- Utworzyć zasadę ochrony dla stacji roboczych i serwerów, a także zadania skanowania w poszukiwaniu złośliwego oprogramowania, zadania pobierania uaktualnień i zadania tworzenia kopii zapasowej danych dla najwyższego poziomu hierarchii zarządzanych urządzeń. Po zakończeniu pracy kreatora wstępnej konfiguracji, utworzone zadania są wyświetlane na liście **Serwer administracyjny → Zadania**, zasady odpowiadające wtyczkom dla zarządzanych aplikacji są wyświetlane na liście **Serwer administracyjny → Zasady**.

Kreator wstępnej konfiguracji tworzy zasady dla zarządzanych aplikacji, takich jak Kaspersky Endpoint Security for Windows, dopóki te zasady nie zostały już utworzone dla grupy **Zarządzane urządzenia**. Kreator wstępnej konfiguracji tworzy zadania, jeśli zadania z tymi samymi nazwami nie istnieją dla grupy **Zarządzane urządzenia**.

W Konsoli administracyjnej Kaspersky Security Center automatycznie wyświetli pytanie o uruchomienie kreatora wstępnej konfiguracji po uruchomieniu go po raz pierwszy. Kreator wstępnej konfiguracji można również uruchomić ręcznie w dowolnym momencie.

Uruchamianie kreatora wstępnej konfiguracji Serwera administracyjnego

Po zainstalowaniu Serwera administracyjnego, przy pierwszym nawiązaniu połączenia z nim, aplikacja automatycznie wyświetli pytanie dotyczące uruchomienia kreatora wstępnej konfiguracji. Kreator wstępnej konfiguracji można również uruchomić ręcznie w dowolnym momencie.

W celu ręcznego uruchomienia kreatora wstępnej konfiguracji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.

2. Z menu kontekstowego węzła wybierz **Wszystkie zadania → Kreator wstępnej konfiguracji Serwera administracyjnego**.

kreator wyświetli pytanie o przeprowadzenie wstępnej konfiguracji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

Jeśli ponownie uruchomisz Kreator wstępnej konfiguracji, zadania i zasady utworzone przy poprzednim uruchomieniu kreatora nie mogą zostać ponownie utworzone.

Krok 1. Konfigurowanie serwera proxy

Określ ustawienia dostępu do Internetu dla Serwera administracyjnego. Należy skonfigurować dostęp do Internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji Kaspersky.

Wybierz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest wybrana, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

- **Adres**

  Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

- **Numer portu**

  Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

- **Pomiń serwer proxy dla adresów lokalnych**

  Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

- **Nazwa użytkownika**

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

- **Hasło**

  Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

  Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Możesz skonfigurować dostęp do Internetu później, niezależnie od kreatora wstępnej konfiguracji.

Krok 2. Wybieranie metody aktywacji aplikacji

Wybierz jedną z poniższych opcji aktywacji Kaspersky Security Center:

- **Wprowadzając kod aktywacyjny**

  Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Możesz wprowadzić kod aktywacyjny w celu dodania klucza aktywującego Kaspersky Security Center. Możesz otrzymać kod aktywacyjny na adres e-mail, który określiłeś po zakupieniu Kaspersky Security Center.

  Aby aktywować aplikację kodem aktywacyjnym, potrzebny jest dostęp do internetu w celu nawiązania połączenia z serwerami aktywacji Kaspersky.

  Jeśli wybrałeś tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w węźle **Licencje Kaspersky** drzewa Konsoli administracyjnej.

- **Określając plik klucza**

  Plik klucza to plik z rozszerzeniem .key, dostarczony przez firmę Kaspersky. Plik klucza jest przeznaczony do dodania klucza aktywującego aplikację.

  Możesz otrzymać plik klucza na adres e-mail, który określiłeś po zakupieniu Kaspersky Security Center.

  Aby aktywować aplikację przy pomocy pliku klucza, nie musisz łączyć się z serwerami aktywacji Kaspersky.

  Jeśli wybrałeś tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w węźle **Licencje Kaspersky** drzewa Konsoli administracyjnej.

- **Odraczając aktywację aplikacji**

  Aplikacja będzie działała z podstawową funkcjonalnością, bez Zarządzania urządzeniami mobilnymi oraz bez Zarządzania systemami.

Jeśli wybierzesz opcję odroczenia aktywacji aplikacji, będziesz mógł dodać klucz licencyjny w późniejszym czasie.

Krok 3. Wybór obszarów ochrony i systemów operacyjnych

Wybierz obszary ochrony i systemy operacyjne używane w Twojej sieci. Jeśli wybierzesz te opcje, określ filtry dla wtyczek zarządzających aplikacjami i pakietami dystrybucyjnymi na serwerach Kaspersky, które możesz pobrać do zainstalowania na urządzeniach klienckich w Twojej sieci. Wybierz opcje:

- Obszary

  Możesz wybrać następujące obszary ochrony:

  - **Stacje robocze**. Wybierz tę opcję, jeśli chcesz chronić stacje robocze w swojej sieci. Domyślnie zaznaczona jest opcja Stacja robocza.
  - **Serwery plików i magazyny**. Wybierz tę opcję, jeśli chcesz chronić serwery plików w swojej sieci.
  - **Urządzenia mobilne**. Wybierz tę opcję, jeśli chcesz chronić urządzenia mobilne należące do firmy lub pracowników firmy. Jeśli wybierzesz tę opcję, ale nie dostarczyłeś licencji z funkcją Zarządzanie urządzeniami mobilnymi, zostanie wyświetlona wiadomość informująca o konieczności dostarczenia licencji z funkcją Zarządzanie urządzeniami mobilnymi. Jeśli nie dostarczysz licencji, nie możesz korzystać z funkcji Urządzenia mobilne.
  - **Wirtualizacja**. Wybierz tę opcję, jeśli chcesz chronić maszyny wirtualne w swojej sieci.
  - **Kaspersky Anti-Spam**. Wybierz tę opcję, jeśli chcesz chronić serwery pocztowe w swojej organizacji przed spamem, szkodliwymi programami i oszukańczymi wiadomościami.
  - **Systemy wbudowane**. Wybierz tę opcję, jeśli chcesz chronić wbudowane systemy Windows, takie jak bankomat.
  - **Sieci przemysłowe**. Wybierz tę opcję, jeśli chcesz monitorować dane bezpieczeństwa w sieci przemysłowej oraz z punktów końcowych sieci, które są chronione przez aplikacje firmy Kaspersky.
  - **Przemysłowe punkty końcowe**. Wybierz tę opcję, jeśli chcesz chronić pojedyncze węzły w sieci przemysłowej.

- Systemy operacyjne

  Możesz wybrać następujące platformy:

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - Inne

  Informacje na temat obsługiwanych systemów operacyjnych można znaleźć na stronie Wymagania sprzętowe i programowe.

Możesz wybrać pakiety aplikacji Kaspersky z listy dostępnych pakietów później, niezależnie od kreatora wstępnej konfiguracji. Aby uprościć wyszukiwanie potrzebnych pakietów, możesz przefiltrować listę dostępnych pakietów według następujących kryteriów:

- Obszar ochronny

- Rodzaj pobranego oprogramowania (pakiet dystrybucyjny, narzędzie, wtyczka lub wtyczka sieciowa)
- Wersja aplikacji Kaspersky
- Język lokalizacji aplikacji Kaspersky

Krok 4. Wybieranie wtyczek dla zarządzanych aplikacji

Wybierz wtyczki dla zarządzanych aplikacji, które mają zostać zainstalowane. Zostanie wyświetlona lista wtyczek znajdujących się na serwerach Kaspersky. Lista jest filtrowana zgodnie z opcjami wybranymi w poprzednim kroku kreatora. Domyślnie, pełna lista zawiera wtyczki we wszystkich językach. Aby wyświetlić tylko wtyczkę w określonym języku, wybierz język z listy rozwijalnej **Wskaż język dla Konsoli administracyjnej lub**. Lista wtyczek zawiera następujące kolumny:

- **Nazwa aplikacji**

  Zostały wybrane wtyczki zależne od obszarów ochrony i platform, które wybrano w poprzednim kroku.

- **Wersja aplikacji**

  Lista zawiera wtyczki we wszystkich wersjach umieszczone na serwerach Kaspersky. Domyślnie zostaną wybrane wtyczki w najnowszych wersjach.

- **Wersja językowa**

  Domyślnie wersja językowa wtyczki jest definiowana przez wersję językową Kaspersky Security Center, którą wybrałeś w momencie instalacji. Możesz określić inne wersje językowe na liście rozwijalnej **Wskaż język dla Konsoli administracyjnej lub**.

Po wybraniu wtyczek ich instalacja rozpoczyna się automatycznie w oddzielnym oknie. Aby zainstalować niektóre wtyczki, należy zaakceptować warunki Umowy licencyjnej. Zapoznaj się z treścią Umowy licencyjnej, wybierz opcję **Akceptuję warunki Umowy licencyjnej** i kliknij przycisk **Zainstaluj**. Jeśli nie akceptujesz warunków Umowy licencyjnej, wtyczka nie zostanie zainstalowana.

Po zakończeniu instalacji, zamknij okno instalacji.

Wtyczki do zarządzania można również wybrać później, niezależnie od kreatora wstępnej konfiguracji.

Krok 5. Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych

Kaspersky Endpoint Security for Windows zawiera narzędzia do szyfrowania informacji przechowywanych na urządzeniach klienckich. Aby pobrać pakiet dystrybucyjny Kaspersky Endpoint Security for Windows potrzebny w Twojej organizacji, miej na uwadze ustawodawstwo kraju, w którym znajdują się urządzenia klienckie Twojej organizacji.

W oknie **Typ szyfrowania** wybierz jeden z następujących typów szyfrowania:

- Strong encryption (Silne szyfrowanie) (AES256). Ten typ szyfrowania używa klucza o długości 256 bitów.

- Lite encryption (AES56) (Szyfrowanie podstawowe). Ten typ szyfrowania używa klucza o długości 56 bitów.

Okno **Typ szyfrowania** jest wyświetlane tylko wtedy, gdy jako obszar ochrony wybrałeś **Stacje robocze**, a jako platformę **Microsoft Windows.**

Po wybraniu typu szyfrowania, zostanie wyświetlona lista pakietów dystrybucyjnych obu typów szyfrowania. Pakiet dystrybucyjny z wybranym typem szyfrowania zostanie wybrany z listy. Język pakietu dystrybucyjnego odpowiada językowi Kaspersky Security Center. Jeśli wersja językowa pakietu dystrybucyjnego Kaspersky Endpoint Security for Windows dla Kaspersky Security Center nie istnieje, zostanie wybrana angielska wersja językowa pakietu dystrybucyjnego.

Na liście możesz wybrać wersje językowe pakietów dystrybucyjnych, korzystając z listy rozwijalnej **Wskaż język dla Konsoli administracyjnej lub**.

Dystrybutory zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center.

Na liście możesz wybrać pakiet dystrybucyjny dowolnego typu szyfrowania, inny od tego wybranego w oknie **Typ szyfrowania**. Po wybraniu pakietu dystrybucyjnego Kaspersky Endpoint Security for Windows, rozpocznie się pobieranie pakietów dystrybucyjnych odpowiadających komponentom i platformom. Możesz monitorować proces pobierania w kolumnie **Stan pobierania**. Po zakończeniu pracy Kreatora wstępnej konfiguracji, pakiety instalacyjne Agenta sieciowego dla systemu for Windows i zarządzanych aplikacji firmy Kaspersky są wyświetlane na liście **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

Aby zakończyć pobieranie niektórych pakietów dystrybucyjnych, należy zaakceptować Umowę licencyjną. Jeśli klikniesz przycisk **Zaakceptuj**, zostanie wyświetlona treść Umowy licencyjnej. Aby przejść do kolejnego kroku kreatora, należy zaakceptować warunki i postanowienia Umowy licencyjnej oraz warunki i postanowienia Polityki prywatności Kaspersky. Wybierz opcje dotyczące Umowy licencyjnej i Polityki prywatności Kaspersky, a następnie kliknij przycisk **Zaakceptuj wszystkie**. Jeśli nie akceptujesz warunków i postanowień, pobieranie pakietu zostanie anulowane.

Po zaakceptowaniu warunków i postanowień Umowy licencyjnej oraz warunków i postanowień Polityki prywatności Kaspersky, pobieranie pakietów dystrybucyjnych będzie kontynuowane. Jeśli pobieranie zostanie zakończone, zostanie wyświetlony stan **Utworzono pakiet instalacyjny**. W późniejszym czasie możesz wykorzystać pakiety instalacyjne do wdrożenia aplikacji Kaspersky na urządzeniach klienckich.

Pakiety instalacyjne można tworzyć ręcznie, niezależnie od kreatora wstępnej konfiguracji. Przejdź do **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne** w drzewie Konsoli administracyjnej.

Krok 6. Konfigurowanie użycia Kaspersky Security Network

Możesz uzyskać dostęp do baz danych reputacji Kaspersky Security Network, aby zapewnić szybsze reakcje aplikacji Kaspersky na zagrożenia, poprawić skuteczność niektórych komponentów ochrony i zmniejszyć ryzyko fałszywych alarmów.

Przeczytaj Oświadczenie KSN, które zostanie wyświetlone w oknie. Określ ustawienia przekazywania informacji o działaniach Kaspersky Security Center do bazy wiedzy Kaspersky Security Network. Wybierz jedną z następujących opcji:

- **Zgadzam się na korzystanie z Kaspersky Security Network**

Kaspersky Security Center i zarządzane aplikacje zainstalowane na urządzeniach klienckich automatycznie prześlą szczegóły swoich działań do Kaspersky Security Network. Uczestnictwo w Kaspersky Security Network umożliwia szybsze aktualizowanie baz danych zawierających informacje o wirusach i innych zagrożeniach, co zapewnia szybszą reakcję na pojawiające się zagrożenia bezpieczeństwa.

- **Nie zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje nie dostarczą informacji do Kaspersky Security Network.

  Jeśli wybierzesz tę opcję, korzystanie z Kaspersky Security Network zostanie wyłączone.

Jeśli pobrano wtyczkę Kaspersky Endpoint Security for Windows, wyświetlane są oba Oświadczenia KSN — Oświadczenie KSN dla Kaspersky Security Center oraz Oświadczenie KSN dla Kaspersky Endpoint Security for Windows. Oświadczenia KSN dla innych zarządzanych aplikacji firmy Kaspersky, których wtyczki zostały pobrane, są wyświetlane w oddzielnych oknach i każe oświadczenie powinno być zaakceptowane (lub nie) oddzielnie.

Możesz także skonfigurować dostęp Serwera administracyjnego do Kaspersky Security Network (KSN) później w oknie właściwości Serwera administracyjnego Konsoli administracyjnej.

Krok 7. Konfigurowanie powiadomień e-mail

Skonfiguruj wysyłanie powiadomień o zdarzeniach zarejestrowanych podczas działania aplikacji firmy Kaspersky na zarządzanych urządzeniach. Ustawienia te będą używane jako ustawienia domyślne dla Serwera administracyjnego.

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w aplikacjach firmy Kaspersky użyj następujących ustawień:

- **Adresaci (adresy e-mail)**

  Adresy e-mail użytkowników, którym aplikacja będzie wysyłała powiadomienia. Możesz wprowadzić jeden lub więcej adresów; jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami.

- **Serwer SMTP**

  Adres lub adresy serwerów pocztowych Twojej organizacji.

  Jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami. Możesz użyć następujących wartości:

  - Adres IPv4 lub IPv6
  - Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
  - Nazwa DNS serwera SMTP

- **Port serwera SMTP**

  Numer portu komunikacji serwera SMTP. Jeśli korzystasz z kilku serwerów SMTP, połączenie z nimi jest nawiązywane przez określony port komunikacyjny. Domyślny numer portu to 25.

- **Użyj uwierzytelniania ESMTP**

Włącza obsługę autoryzacji ESMTP. Po zaznaczeniu opcji, w polach **Nazwa użytkownika** i **Hasło** możesz określić ustawienia autoryzacji ESMTP. Domyślnie pole to nie jest zaznaczone.

- **Ustawienia**

  Określ następujące ustawienia:

  - **Temat** (podmiot wiadomości e-mail)
  - **Adres e-mail nadawcy**
  - **Ustawienia TLS dla serwera SMTP**

  Możesz określić ustawienia TLS dla serwera SMTP:

  Możesz wyłączyć korzystanie z TLS, użyć TLS, jeśli serwer SMTP obsługuje ten protokół lub możesz wymusić użycie tylko TLS. Jeśli zdecydujesz się używać tylko TLS, określ certyfikat do uwierzytelniania serwera SMTP i wybierz, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Dodatkowo, jeśli wybierzesz używanie tylko TLS, możesz określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

  - Odszukaj plik certyfikatu serwera SMTP:

  Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

  - Odszukaj plik certyfikatu klienta:

  Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

  - Certyfikat X-509:

  Określ plik z certyfikatem oraz plik z kluczem prywatnym. Możesz przesyłać te pliki w dowolnej kolejności. Po przesłaniu obu plików podaj hasło do odszyfrowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

  - Kontener pkcs12:

  Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

Możesz przetestować nowe ustawienia powiadomień e-mail, klikając przycisk **Wyślij wiadomość testową**.

Powiadomienia o zdarzeniach można skonfigurować później, niezależnie od kreatora wstępnej konfiguracji.

Krok 8. Konfigurowanie zarządzania aktualizacją

Skonfiguruj ustawienia zarządzania uaktualnieniami aplikacji zainstalowanych na urządzeniach klienckich.

Możesz skonfigurować te ustawienia tylko wtedy, gdy dostarczyłeś klucz licencyjny z opcją Zarządzanie lukami i poprawkami.

W grupie ustawień **Wyszukiwanie aktualizacji oraz ich instalacja** możesz wybrać tryb wyszukiwania i instalacji uaktualnień Kaspersky Security Center:

- **Wyszukaj wymagane aktualizacje**

  Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie utworzone.

  Opcja ta jest wybrana domyślnie.

- **Wyszukaj i zainstaluj wymagane aktualizacje**

  Zadania *Wyszukiwanie luk i wymaganych aktualizacji* i *Zainstaluj wymagane aktualizacje i napraw luki* są tworzone automatycznie, jeśli ich nie ma.

W grupie ustawień **Windows Server Update Services** możesz wybrać źródło synchronizacji aktualizacji:

- **Użyj źródeł aktualizacji zdefiniowanych w zasadzie domeny**

  Urządzenia klienckie pobiorą aktualizacje Windows Update zgodnie z ustawieniami zasad domeny. Zasada Agenta sieciowego jest tworzona automatycznie, jeśli jeszcze jej nie masz.

- **Użyj Serwera administracyjnego jako serwera WSUS**

  Urządzenia klienckie pobiorą aktualizacje Windows Update z Serwera administracyjnego. Zadanie *Wykonaj synchronizację Windows Update* i zasada Agenta sieciowego są tworozne automatycznie, jeśli jeszcze ich nie masz.

Zadania *Wyszukiwanie luk i wymaganych aktualizacji* oraz *Zainstaluj wymagane aktualizacje i napraw luki* możesz utworzyć niezależnie od kreatora wstępnej konfiguracji. Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie Wykonaj synchronizację *Windows Update* i wybierz opcję **Użyj Serwera administracyjnego jako serwera WSUS** jako serwera WSUS w zasadzie Agenta sieciowego.

Krok 9. Wstępne konfigurowanie ochrony

Okno **Konfiguracja wstępnej ochrony** wyświetla listę profili i zadań, które są tworzone automatycznie. Tworzone są następujące profile i zadania:

- Profil Agenta sieciowego Kaspersky Security Center
- Zasady dla zarządzanych aplikacji firmy Kaspersky, których wtyczki zarządzające zostały zainstalowane wcześniej
- Zadanie Konserwacja Serwera administracyjnego
- Zadanie Kopia zapasowa danych Serwera administracyjnego
- Zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego

- Zadanie Wyszukiwanie luk i wymaganych aktualizacji
- Zadanie Zainstaluj aktualizację

Przed przystąpieniem do następnego kroku kreatora poczekaj na zakończenie tworzenia zasad i zadań.

Jeśli pobrałeś i zainstalowałeś wtyczkę dla Kaspersky Endpoint Security for Windows 10 Service Pack 1 i nowszej wersji, aż do wersji 11.0.1, podczas tworzenia profili i zadań zostanie otwarte okno dla wstępnej konfiguracji strefy zaufanej Kaspersky Endpoint Security for Windows. Aplikacja poprosi o dodanie producentów, którzy zostali zweryfikowani przez Kaspersky, do strefy zaufanej w celu wykluczenia ich aplikacji ze skanowania, aby zapobiec ich przypadkowemu zablokowaniu. Możesz teraz utworzyć zalecane wykluczenia lub utworzyć listę wykluczeń w późniejszym czasie, wybierając następujące elementy w drzewie konsoli: **Profile** → Menu właściwości Kaspersky Endpoint Security → **Zaawansowana ochrona przed zagrożeniami** → **Strefa zaufana** → **Ustawienia** → **Dodaj**. Lista wykluczeń ze skanowania jest dostępna do edycji w dowolnym momencie podczas korzystania z aplikacji.

> Działania na strefie zaufanej są wykonywane przy użyciu narzędzi zintegrowanych z Kaspersky Endpoint Security for Windows. Szczegółowe instrukcje dotyczące wykonywania działań oraz opis funkcji szyfrowania są dostępne w internetowym systemie pomocy dla Kaspersky Endpoint Security for Windows.

W celu zakończenia wstępnej konfiguracji strefy zaufanej i powrotu do kreatora kliknij **OK**.

Kliknij **Dalej**. Ten przycisk jest dostępny po utworzeniu wszystkich niezbędnych profili i zadań.

Wymagane zadania i zasady można również utworzyć później, niezależnie od kreatora wstępnej konfiguracji.

Krok 10. Podłączanie urządzeń mobilnych

Jeśli wcześniej włączono obszar ochrony **Urządzenia mobilne** w ustawieniach kreatora, określ ustawienia połączenia firmowych urządzeń mobilnych zarządzanej organizacji. Jeśli nie włączyłeś obszaru ochrony **Urządzenia mobilne**, ten krok jest pomijany.

W tym kroku kreatora należy wykonać następujące czynności:

- Skonfigurować porty dla połączenia urządzeń mobilnych
- Skonfigurować uwierzytelnianie Serwera administracyjnego
- Utworzyć lub zarządzać certyfikatami
- Skonfigurować wydawanie, automatyczne aktualizowanie i szyfrowanie certyfikatów ogólnego typu
- Utworzyć regułę przenoszenia dla urządzeń mobilnych

W celu ustawienia portów dla połączenia urządzeń mobilnych:

1. Kliknij przycisk **Konfiguruj** po prawej stronie pola **Połączenie urządzenia mobilnego**.
2. Z listy rozwijalnej wybierz **Konfiguruj porty**.
   Zostanie otwarte okno właściwości Serwera administracyjnego, wyświetlające sekcję **Porty dodatkowe**.
3. W sekcji **Porty dodatkowe** możesz określić ustawienia połączenia urządzenia mobilnego:
   - Port SSL do aktywacji przy użyciu serwera proxy

Numer portu SSL do połączenia Kaspersky Endpoint Security for Windows z serwerami aktywacji Kaspersky.

Domyślny numer portu to 17000.

- **Otwórz port dla urządzeń mobilnych**

  Port zostaje otwarty dla urządzeń mobilnych do połączenia z serwerem licencjonowania. Możesz zdefiniować numer portu i inne ustawienia w polach poniżej.

  Domyślnie opcja ta jest włączona.

- **Port do synchronizacji urządzeń mobilnych**

  Numer portu, za pomocą którego urządzenia mobilne będą łączyć się z Serwerem administracyjnym i będą wymieniać z nim dane. Domyślny numer portu to 13292.

  Jeśli port 13292 jest używany do innych celów, można przypisać inny port.

- **Port do aktywacji urządzeń mobilnych**

  Port do łączenia Kaspersky Endpoint Security for Android z serwerami aktywacji Kaspersky.

  Domyślny numer portu to 17100.

- **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

  Urządzenia chronione UEFI mogą nawiązywać połączenie z Serwerem administracyjnym.

- **Port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

  Możesz zmienić numer portu, jeśli opcja **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS** jest włączona. Domyślny numer portu to 13294.

4. Kliknij **OK**, aby zapisać zmiany i powrócić do kreatora wstępnej konfiguracji.

Musisz skonfigurować autoryzację Serwera administracyjnego przez urządzenia mobilne i autoryzację urządzeń mobilnych przez Serwer administracyjny. Jeśli chcesz, możesz skonfigurować autoryzację później, oddzielnie od kreatora wstępnej konfiguracji.

W celu skonfigurowania autoryzacji Serwera administracyjnego przez urządzenia mobilne:

1. Kliknij przycisk **Konfiguruj** po prawej stronie pola **Połączenie urządzenia mobilnego**.
2. Z listy rozwijalnej wybierz **Konfiguruj uwierzytelnianie**.

   Zostanie otwarte okno właściwości Serwera administracyjnego, wyświetlające sekcję **Certyfikaty**.
3. Wybierz opcję uwierzytelniania dla urządzeń mobilnych w grupie ustawień **Uwierzytelnianie Serwera administracyjnego przez urządzenia mobilne** i wybierz opcję uwierzytelniania dla urządzeń chronionych UEFI w grupie ustawień **Uwierzytelnianie Serwera administracyjnego przez urządzenia chronione UEFI**.

   Jeśli Serwer administracyjny wymienia dane z urządzeniami klienckimi, jest uwierzytelniany za pomocą certyfikatu.

Domyślnie Serwer administracyjny używa certyfikatu, który został utworzony podczas instalacji Serwera administracyjnego. Jeśli chcesz, możesz dodać nowy certyfikat.

W celu dodania nowego certyfikatu (opcjonalnie):

1. Wybierz **Inny certyfikat**.

   Pojawi się przycisk **Przeglądaj**.

2. Kliknij przycisk **Przeglądaj**.

3. W otwartym oknie określ ustawienia certyfikatu:

   - Typ certyfikatu

     Z listy rozwijalnej możesz wybrać typ certyfikatu:

     - **Certyfikat X.509**. Jeśli ta opcja jest zaznaczona, powinieneś określić prywatny klucz certyfikatu oraz otworzyć certyfikat:

       - **Klucz prywatny (.prk, .pem)**. W tym polu kliknij przycisk **Przeglądaj**, aby określić prywatny klucz certyfikatu w formacie PKCS #8 (*.prk).

       - **Klucz publiczny (.cer)**. W tym polu kliknij przycisk **Przeglądaj**, aby określić publiczny klucz certyfikatu w formacie PEM (*.cer).

     - **Kontener PKCS #12**. Jeśli wybierzesz tę opcję, możesz określić plik certyfikatu w formacie P12 lub PFX, klikając przycisk **Przeglądaj** i uzupełniając pole **Plik certyfikatu**.

   - Czas aktywacji:

     - Natychmiast

       Po kliknięciu **OK**, bieżący certyfikat zostanie natychmiast zastąpiony nowym.

       Wcześniej podłączone urządzenia mobilne nie będą mogły nawiązać połączenia z Serwerem administracyjnym.

     - Po wygaśnięciu tego okresu, dni

       Jeśli wybierzesz tę opcję, zostanie wygenerowany certyfikat zapasowy. Bieżący certyfikat zostanie zastąpiony nowym w ciągu określonej liczby dni. Data obowiązywania certyfikatu zapasowego jest wyświetlona w sekcji **Certyfikaty**.

       Zalecane jest zaplanowanie ponownej publikacji w przyszłości. Certyfikat rezerwowy należy pobrać na urządzenia mobilne przed upływem określonego terminu. Po zastąpieniu bieżącego certyfikatu nowym, wcześniej podłączone urządzenia mobilne, na których nie ma zapasowego certyfikatu, nie będą mogły nawiązać połączenia z Serwerem administracyjnym.

4. Kliknij przycisk **Właściwości**, aby wyświetlić ustawienia wybranego certyfikatu Serwera administracyjnego.

W celu ponownego wydania certyfikatu poprzez Serwer administracyjny:

1. Wybierz **Certyfikat wydany przez Serwer administracyjny**.

2. Kliknij przycisk **Wydaj ponownie**.

3. W otwartym oknie określ następujące ustawienia:

   - Adres połączenia:

     - **Użyj poprzedniego adresu połączenia**

       Adres Serwera administracyjnego, z którym łączą się urządzenia mobilne, pozostają niezmienione.

       Opcja ta jest wybrana domyślnie.

     - **Zmień adres połączenia na**

       Jeśli chcesz, żeby urządzenia mobilne nawiązywały połączenie z innym adresem, w tym polu określ odpowiedni adres.

       Jeśli adres dla podłączania urządzeń mobilnych został zmieniony, należy wydać nowy certyfikat. Stary certyfikat staje się nieważny na wszystkich podłączonych urządzeniach mobilnych. Poprzednio podłączone urządzenia nie będą mogły nawiązać połączenia z Serwerem administracyjnym, więc staną się niezarządzane.

   - Czas aktywacji:

     - **Natychmiast**

       Po kliknięciu **OK**, bieżący certyfikat zostanie natychmiast zastąpiony nowym.

       Wcześniej podłączone urządzenia mobilne nie będą mogły nawiązać połączenia z Serwerem administracyjnym.

     - **Po wygaśnięciu tego okresu, dni**

       Jeśli wybierzesz tę opcję, zostanie wygenerowany certyfikat zapasowy. Bieżący certyfikat zostanie zastąpiony nowym w ciągu określonej liczby dni. Data obowiązywania certyfikatu zapasowego jest wyświetlona w sekcji **Certyfikaty**.

       Zalecane jest zaplanowanie ponownej publikacji w przyszłości. Certyfikat rezerwowy należy pobrać na urządzenia mobilne przed upływem określonego terminu. Po zastąpieniu bieżącego certyfikatu nowym, wcześniej podłączone urządzenia mobilne, na których nie ma zapasowego certyfikatu, nie będą mogły nawiązać połączenia z Serwerem administracyjnym.

4. Kliknij **OK**, aby zapisać zmiany i powrócić do okna **Certyfikaty**.

5. Kliknij **OK**, aby zapisać zmiany i powrócić do kreatora wstępnej konfiguracji.

W celu skonfigurowania wydawania, automatycznej aktualizacji i szyfrowania certyfikatów ogólnego typu dla identyfikacji urządzeń mobilnych przez Serwer administracyjny:

1. Kliknij przycisk **Konfiguruj** po prawej stronie pola **Autoryzacja urządzenia mobilnego**.

   Zostanie otwarte okno **Reguły wydawania certyfikatu** wyświetlające sekcję **Wydawanie certyfikatów dla urządzeń mobilnych**.

2. W razie potrzeby określ następujące ustawienia w sekcji **Ustawienia wydawania**:

   - **Okres ważności certyfikatu, dni**

Okres ważności certyfikatu w dniach. Domyślny czas życia certyfikatu wynosi 365 dni. Po upływie tego okresu, urządzenie mobilne nie będzie mogło połączyć się z Serwerem administracyjnym.

- **Źródło certyfikatu**

  Wybierz źródło certyfikatów ogólnego typu dla urządzeń mobilnych: certyfikaty są wydawane przez Serwer administracyjny lub są określane ręcznie.

  Szablony certyfikatów można zmodyfikować, jeśli integracja z infrastrukturą kluczy publicznych (PKI) została skonfigurowana w sekcji **Integracja z PKI**. W takim przypadku dostępne są następujące pola wyboru szablonu:

- **Szablon domyślny**

  Użyj certyfikatu wystawionego przez zewnętrzne źródło certyfikatu - Centrum certyfikacji - pod domyślnym szablonem.

  Domyślnie opcja ta jest zaznaczona.

- **Inny szablon**

  Wybierz szablon używany do wydawania certyfikatów. Możesz określić szablony certyfikatów w domenie. Przycisk **Odśwież listę** zaktualizuje listę szablonów certyfikatów.

3. Jeśli to konieczne, określ następujące ustawienia automatycznego wystawiania certyfikatów w sekcji **Ustawienia aktualizacji automatycznych**:

   - **Odnów, gdy certyfikat wygaśnie za (dni)**

     Liczba dni pozostałych do wygaśnięcia bieżącego certyfikatu, w trakcie których Serwer administracyjny powinien opublikować nowy certyfikat. Na przykład, jeśli wartość pola to 4, Serwer administracyjny opublikuje nowy certyfikat na cztery dni przed wygaśnięciem bieżącego certyfikatu. Domyślna wartość to 7.

   - **Odnów certyfikat automatycznie, jeśli jest to możliwe**

     Wybierz tę opcję, aby automatycznie ponownie wystawić certyfikat na liczbę dni określoną w polu **Odnów, gdy certyfikat wygaśnie za (dni)**. Jeśli certyfikat został zdefiniowany ręcznie, nie można go automatycznie odnowić, a włączona opcja nie będzie działać.

     Domyślnie opcja ta jest wyłączona.

   Certyfikaty są automatycznie ponownie publikowane przez Urząd certyfikacji.

4. Jeśli to konieczne, w sekcji ustawień **Ochrona hasłem** określ ustawienia do odszyfrowywania certyfikatów podczas instalacji.

   Wybierz opcję **Pytaj o hasło podczas instalowania certyfikatów**, aby zażądać hasła użytkownika, jeśli certyfikat jest zainstalowany na urządzeniu mobilnym. Hasło jest używane tylko raz, podczas instalacji certyfikatu na urządzeniu mobilnym.

Hasło zostanie wygenerowane automatycznie przez Serwer administracyjny i wysłane na podany adres e-mail. Możesz podać adres e-mail użytkownika lub własny adres e-mail, jeśli chcesz użyć innej metody przekazywania hasła do użytkownika.

Możesz użyć suwaka, aby określić liczbę znaków w haśle do odszyfrowywania certyfikatów.

Opcja wyświetlania hasła jest wymagana, na przykład, w celu ochrony certyfikatu współdzielonego w autonomicznym pakiecie instalacyjnym Kaspersky Endpoint Security for Android. Ochrona hasłem uniemożliwia intruzowi uzyskanie dostępu do certyfikatu współdzielonego poprzez kradzież autonomicznego pakietu instalacyjnego z Kaspersky Security Center Web Server.

Jeśli to pole jest wyłączone, certyfikat zostanie automatycznie odszyfrowany podczas instalacji, a użytkownik nie będzie pytany o hasło. Domyślnie opcja ta jest wyłączona.

5. Kliknij **OK**, aby zapisać zmiany i powrócić do okna kreatora wstępnej konfiguracji.

   Kliknij przycisk **Anuluj**, aby powrócić do kreatora wstępnej konfiguracji bez zapisywania jakichkolwiek zmian.

W celu włączenia funkcji przenoszenia urządzeń mobilnych do grupy administracyjnej, którą wybierzesz,

W polu **Automatyczne przenoszenie urządzeń mobilnych** wybierz opcję **Utwórz regułę przenoszenia dla urządzeń mobilnych**.

Jeśli opcja **Utwórz regułę przenoszenia dla urządzeń mobilnych** jest wybrana, aplikacja automatycznie tworzy regułę przenoszenia, która przenosi urządzenia działające pod systemem Android i iOS do grupy **Zarządzane urządzenia**:

- Z systemami operacyjnymi Android, na których zainstalowany jest Kaspersky Endpoint Security for Android oraz certyfikat dla urządzeń mobilnych
- Z systemami operacyjnymi iOS, na których zainstalowany jest profil iOS MDM oraz certyfikat współdzielony

Jeśli taka reguła już istnieje, aplikacja nie tworzy jej ponownie.

Domyślnie opcja ta jest wyłączona.

Kaspersky nie wspiera już Kaspersky Safe Browser.

Krok 11. Pobieranie aktualizacji

Aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky są pobierane automatycznie. Aktualizacje są pobierane z serwerów Kaspersky.

Aby pobierać aktualizacje niezależnie od kreatora wstępnej konfiguracji, utwórz i skonfiguruj zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

Krok 12. Wykrywanie urządzeń

Okno **Przeszukiwanie sieci** wyświetla informacje o stanie przeszukiwania sieci wykonywanym przez Serwer administracyjny.

Możesz wyświetlić urządzenia sieciowe wykryte przez Serwer administracyjny i uzyskać pomoc na temat pracy z oknem **Wykrywanie urządzeń**, klikając odnośniki w dolnej części okna.

Możesz wykonać przeszukiwanie sieci później, niezależnie od kreatora wstępnej konfiguracji. Użyj Konsoli administracyjnej, aby skonfigurować przeszukiwanie domen Windows, Active Directory, zakresów IP i sieci IPv6.

Krok 13. Zamykanie kreatora wstępnej konfiguracji

W oknie zakończenia pracy Kreatora wstępnej konfiguracji wybierz opcję **Tworzenie zadania zdalnej instalacji**, jeśli chcesz uruchomić automatyczną instalację aplikacji antywirusowych i/lub Agenta sieciowego na urządzeniach w sieci.

Aby zakończyć działanie kreatora, kliknij przycisk **Zakończ**.

Konfigurowanie połączenia Konsoli administracyjnej z Serwerem administracyjnym

Konsola administracyjna jest połączona z Serwerem administracyjnym poprzez port SSL TCP 13291. Ten sam port może być używany przez obiekty automatyzacji klakaut.

Port TCP o numerze 14000 może być używany do podłączania Konsoli administracyjnej, punktów dystrybucji, podrzędnych Serwerów administracyjnych i obiektów narzędzia klakaut, a także do pobierania danych z urządzeń klienckich.

Zazwyczaj, Port TCP o numerze 13000 dla protokołu SSL może być używany tylko przez Agenta sieciowego, podrzędny Serwer administracyjny i główny Serwer administracyjny w DMZ. W niektórych przypadkach konieczne może być podłączenie Konsoli administracyjnej za pośrednictwem portu SSL o numerze 13000:

- Jeśli pojedynczy port SSL będzie używany dla Konsoli administracyjnej i do innych działań (pobierania danych z urządzeń klienckich, podłączania punktów dystrybucji lub podłączania podrzędnych Serwerów administracyjnych).
- Jeśli obiekt narzędzia klakaut nie jest podłączany bezpośrednio do Serwera administracyjnego, ale za pośrednictwem punktu dystrybucji w DMZ.

W celu zezwolenia na łączenie Konsoli administracyjnej za pośrednictwem portu 13000:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).
2. Przejdź do gałęzi:
   - W systemach 32-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - W systemach 64-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Dla klucza LP_ConsoleMustUsePort13291 (DWORD) ustaw wartość 00000000.
   1 jest domyślną wartością określoną dla tego klucza.
4. Uruchom ponownie usługę Serwera administracyjnego.

Teraz możliwe będzie połączenie Konsoli administracyjnej z Serwerem administracyjnym za pośrednictwem portu 13000.

Konfigurowanie ustawień dostępu do Internetu dla Serwera administracyjnego

Należy skonfigurować dostęp do Internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji Kaspersky.

Aby określić ustawienia dostępu do Internetu dla Serwera administracyjnego:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego przejdź do **Zaawansowane** → **Konfiguracja dostępu do internetu**.
4. Wybierz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest wybrana, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

   - **Adres**

     Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

   - **Numer portu**

     Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

   - **Pomiń serwer proxy dla adresów lokalnych**

     Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

   - **Uwierzytelnianie na serwerze proxy**

     Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

     To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

   - **Nazwa użytkownika**

     Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

   - **Hasło**

Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Dostęp do Internetu można również skonfigurować za pomocą kreatora wstępnej konfiguracji.

Podłączanie urządzeń mobilnych

Ta sekcja opisuje sposób podłączania zarządzanych urządzeń mobilnych (czyli zarządzanych urządzeń znajdujących się poza siecią główną) z Serwerem administracyjnym.

Scenariusz: Podłączanie urządzeń mobilnych przez bramę połączenia

W tym scenariuszu opisano sposób podłączania zarządzanych urządzeń znajdujących się poza siecią główną z Serwerem administracyjnym.

Wymagania wstępne

Scenariusz ma następujące wymagania wstępne:

- Strefa zdemilitaryzowana (DMZ) jest zorganizowana w sieci Twojej organizacji.
- Serwer administracyjny Kaspersky Security Center jest zainstalowany w sieci firmowej.

Etapy

Ten scenariusz przebiega etapami:

1. **Wybieranie urządzenia kliencka w DMZ**

   To urządzenie zostanie użyte jako brama połączenia. Urządzenie, które wybrałeś, musi spełniać wymagania dla bram połączenia.

2. **Instalowanie Agenta sieciowego w roli bramy połączenia**

   Do zainstalowania Agenta sieciowego na wybranym urządzeniu zalecane jest używanie instalacji lokalnej.

   Domyślnie plik instalacyjny znajduje się w następującym miejscu: \\<nazwa serwera>\KLSHARE\PkgInst\NetAgent_<numer wersji>

   W oknie **Brama połączenia** kreatora instalacji Agenta sieciowego wybierz **Użyj Agenta sieciowego jako bramy połączenia w DMZ**. Ten tryb jednocześnie aktywuje rolę bramy połączenia i nakazuje Agentowi sieciowemu czekać na połączenia z Serwera administracyjnego zamiast nawiązywać połączenia z Serwerem administracyjnym.

   Alternatywnie możesz zainstalować Agenta sieciowego na urządzeniu z systemem Linux i skonfigurować Agenta sieciowego do pracy jako brama połączenia, ale zwróć uwagę na listę ograniczeń Agenta sieciowego działającego na urządzeniach z systemem Linux.

3. **Zezwalanie na połączenia w zaporach sieciowych w bramie połączenia**

Aby upewnić się, że Serwer administracyjny może faktycznie połączyć się z bramą połączenia w strefie DMZ, zezwolić na połączenia z portem TCP o numerze 13000 we wszystkich zaporach ogniowych między Serwerem administracyjnym a bramą połączenia.

Jeśli brama połączenia nie ma rzeczywistego adresu IP w Internecie, ale zamiast tego znajduje się poza NAT (Network Address Translation — translacja adresów sieciowych), skonfiguruj regułę, aby przekazywać połączenia przez NAT.

4 Tworzenie grupy administracyjnej dla urządzeń zewnętrznych

Utwórz nową grupę w grupie **Zarządzane urządzenia**. Ta nowa grupa będzie zawierała zewnętrzne zarządzane urządzenia.

5 Podłączanie bramy połączenia do Serwera administracyjnego

Brama połączenia, którą skonfigurowałeś, oczekuje na połączenie z Serwera administracyjnego. Jednakże Serwer administracyjny nie wyświetla urządzenia z bramą połączenia wśród zarządzanych urządzeń. Dzieje się tak ponieważ brama połączenia nie próbowała nawiązać połączenia z Serwerem administracyjnym. Dlatego też należy przeprowadzić specjalną procedurę w celu zapewnienia, że Serwer administracyjny zainicjuje połączenie z bramą połączenia.

Wykonaj następujące czynności:

1. Dodaj bramę połączenia jako punkt dystrybucji.
2. Przenieś bramę połączenia z grupy **Nieprzypisane urządzenia** do grupy utworzonej dla urządzeń zewnętrznych.

Brama połączenia została podłączona i skonfigurowana.

6 Podłączanie zewnętrznych komputerów stacjonarnych do Serwera administracyjnego

Zwykle zewnętrzne komputery stacjonarne nie są przenoszone wewnątrz obwodu. Dlatego musisz skonfigurować je tak, aby łączyły się z Serwerem administracyjnym przez bramę podczas instalowania Agenta sieciowego.

7 Konfigurowanie aktualizacji dla zewnętrznych komputerów stacjonarnych

Jeśli aktualizacje aplikacji zabezpieczających są skonfigurowane do pobierania z Serwera administracyjnego, komputery zewnętrzne pobierają aktualizacje przez bramę połączenia. Ma to dwie wady:

- To niepotrzebny ruch, który zajmuje przepustowość kanału komunikacji internetowej firmy.
- Niekoniecznie jest to najszybszy sposób uzyskiwania aktualizacji. Jest bardzo prawdopodobne, że pobieranie aktualizacji z serwerów aktualizacji Kaspersky byłoby tańsze i szybsze.

Wykonaj następujące czynności:

1. Przenieś wszystkie komputery zewnętrzne do oddzielnej grupy administracyjnej, którą utworzyłeś wcześniej.
2. Wyklucz grupę z urządzeniami zewnętrznymi z zadania aktualizacji.
3. Utwórz osobne zadanie aktualizacji dla grupy z urządzeniami zewnętrznymi.

8 Podłączanie przenośnych laptopów do Serwera administracyjnego

Przenośne laptopy są czasami w sieci, a czasami poza nią. W celu efektywnego zarządzania należy połączyć je z Serwerem administracyjnym w różny sposób w zależności od ich lokalizacji. Aby efektywnie wykorzystywać ruch sieciowy, muszą również pobierać uaktualnienia z różnych źródeł w zależności od ich lokalizacji.

Należy skonfigurować reguły dla użytkowników mobilnych: profile połączeń i opisy lokalizacji sieciowych. Każda reguła definiuje instancję Serwera administracyjnego, z którym muszą łączyć się przenośne laptopy w zależności od ich lokalizacji oraz instancji Serwera administracyjnego, z którego muszą pobierać aktualizacje.

Informacje o podłączaniu urządzeń mobilnych

Niektóre zarządzane urządzenia zawsze znajdują się poza główną siecią (na przykład, komputery w oddziałach regionalnych firmy; kioski, bankomaty i terminale zainstalowane w różnych punktach sprzedaży; komputery w domowych biurach pracowników). Niektóre urządzenia od czasu do czasu wyjeżdżają poza granicę (na przykład, laptopy użytkowników, którzy odwiedzają oddziały regionalne lub biuro klienta).

Nadal musisz monitorować i zarządzać ochroną urządzeń znajdujących się poza biurem - otrzymywać aktualne informacje o ich stanie ochrony i zapewniać aktualność aplikacji zabezpieczających. Jest to konieczne, ponieważ, na przykład, jeśli do takiego urządzenia ktoś się włamał, gdy znajdowało się poza siecią główną, może stać się platformą do rozprzestrzeniania zagrożeń, gdy tylko połączy się z siecią główną. W celu podłączenia urządzeń mobilnych do Serwera administracyjnego, możesz użyć dwóch metod:

- Brama połączenia w strefie zdemilitaryzowanej (DMZ)

  Zobacz schemat transmisji danych: Serwer administracyjny w sieci LAN, zarządzane urządzenia w internecie, używana brama połączenia

- Serwer administracyjny w strefie DMZ

  Zobacz schemat transmisji danych: Serwer administracyjny w strefie DMZ, zarządzane urządzenia w internecie

Brama połączenia w strefie DMZ

Zalecaną metodą podłączania urządzeń mobilnych do Serwera administracyjnego jest zorganizowanie strefy DMZ w sieci organizacji i zainstalowanie bramy połączenia w strefie DMZ. Urządzenia zewnętrzne nawiążą połączenie z bramą połączenia, a Serwer administracyjny znajdujący się w sieci zainicjuje połączenie z urządzeniami za pośrednictwem bramy połączenia.

W porównaniu z drugą metodą ta jest bezpieczniejsza:

- Nie musisz otwierać dostępu do Serwera administracyjnego spoza sieci.
- Uszkodzona brama połączenia nie stwarza dużego zagrożenia dla bezpieczeństwa urządzeń sieciowych. Brama połączeń w rzeczywistości sama niczym nie zarządza i nie ustanawia żadnych połączeń.

Ponadto brama połączeń nie wymaga wielu zasobów sprzętowych.

Jednakże ta metoda ma bardziej skomplikowany proces konfiguracji:

- Aby urządzenie służyło jako brama połączenia w DMZ, musisz zainstalować Agenta sieciowego i podłączyć go do Serwera administracyjnego w określony sposób.
- Nie będziesz mógł używać tego samego adresu do łączenia się z Serwerem administracyjnym we wszystkich sytuacjach. Poza granicami, będziesz musiał użyć nie tylko innego adresu (adresu bramy połączenia), ale także innego trybu połączenia: przez bramę połączenia.
- Musisz także zdefiniować różne ustawienia połączeń dla laptopów w różnych lokalizacjach.

Serwer administracyjny w strefie DMZ

Inną metodą jest zainstalowanie pojedynczego Serwera administracyjnego w strefie DMZ.

Ta konfiguracja jest mniej bezpieczna niż inna metoda. Aby w tym przypadku zarządzać zewnętrznymi laptopami, Serwer administracyjny musi akceptować połączenia z dowolnego adresu w Internecie. Nadal będzie zarządzać wszystkimi urządzeniami w sieci wewnętrznej, ale z DMZ. Dlatego przejęty Serwer może spowodować ogromne szkody, pomimo niskiego prawdopodobieństwa takiego zdarzenia.

Ryzyko jest znacznie niższe, jeśli Serwer administracyjny w DMZ nie zarządza urządzeniami w sieci wewnętrznej. Taka konfiguracja może być wykorzystana, na przykład, przez usługodawcę do zarządzania urządzeniami klientów.

Możesz chcieć użyć tej metody w następujących przypadkach:

- Jeśli jesteś zaznajomiony z instalacją i konfiguracją Serwera administracyjnego i nie chcesz wykonywać innej procedury instalacji i konfiguracji bramy połączenia.
- Jeśli potrzebujesz zarządzać większą liczbą urządzeń. Maksymalna pojemność Serwera administracyjnego to 100 000 urządzeń, podczas gdy brama połączenia może obsługiwać do 10 000 urządzeń.

To rozwiązanie ma również możliwe trudności:

- Serwer administracyjny wymaga większej ilości zasobów sprzętowych i jeszcze jednej bazy danych.
- Informacje o urządzeniach będą przechowywane w dwóch niepowiązanych bazach danych (dla Serwera administracyjnego w sieci i jednej w DMZ), co komplikuje monitorowanie.
- Aby zarządzać wszystkimi urządzeniami, Serwer administracyjny musi być połączony w hierarchię, co komplikuje nie tylko monitorowanie, ale także zarządzanie. Instancja podrzędnego Serwera administracyjnego nakłada ograniczenia na możliwe struktury grup administracyjnych. Musisz zdecydować, w jaki sposób i które zadania i zasady mają być dystrybuowane do instancji podrzędnego Serwera administracyjnego.
- Skonfigurowanie urządzeń zewnętrznych do używania Serwera administracyjnego w DMZ z zewnątrz oraz do używania głównego Serwera administracyjnego od wewnątrz nie jest prostsze niż zwykłe skonfigurowanie ich tak, aby używały warunkowego połączenia przez bramę.
- Wysokie zagrożenia bezpieczeństwa. Zagrożona instancja Serwera administracyjnego ułatwia włamanie się do zarządzanych laptopów. Jeśli tak się stanie, hakerzy muszą tylko poczekać, aż jeden z laptopów wróci do sieci firmowej, aby mogli kontynuować atak na sieć lokalną.

Podłączanie zewnętrznych komputerów stacjonarnych do Serwera administracyjnego

Komputery stacjonarne, które zawsze znajdują się poza główną siecią (na przykład, komputery w oddziałach regionalnych firmy; kioski, bankomaty i terminale zainstalowane w różnych punktach sprzedaży; komputery w domowych biurach pracowników) nie mogą być podłączane bezpośrednio do Serwera administracyjnego. Muszą być podłączeni do Serwera administracyjnego przez bramę połączenia zainstalowaną w strefie zdemilitaryzowanej (DMZ). Ta konfiguracja jest wykonywana podczas instalacji Agenta sieciowego na tych komputerach.

W celu podłączenia zewnętrznych komputerów stacjonarnych do Serwera administracyjnego:

1. Utwórz nowy pakiet instalacyjny dla Agenta sieciowego.
2. Otwórz właściwości utworzonego pakietu instalacyjnego i przejdź do sekcji **Zaawansowane**, a następnie wybierz opcję **Połącz z Serwerem administracyjnym korzystając z bramy połączenia**.

Ustawienie **Połącz z Serwerem administracyjnym korzystając z bramy połączenia** jest niekompatybilne z ustawieniem **Użyj Agenta sieciowego jako bramy połączenia w DMZ**. Nie możesz włączyć obu tych ustawień jednocześnie.

3. W sekcji **Adres bramy połączenia** określ publiczny adres bramy połączenia.

   Jeśli brama połączenia znajduje się za translacją adresów sieciowych (NAT) i nie ma własnego adresu publicznego, skonfiguruj regułę bramy NAT w celu przekazywania połączeń z adresu publicznego na adres wewnętrzny bramy połączenia.

4. Utwórz autonomiczny pakiet instalacyjny w oparciu o utworzony pakiet instalacyjny.

5. Dostarcz autonomiczny pakiet instalacyjny na komputery docelowe elektronicznie lub na dysku wymiennym.

6. Zainstaluj Agenta sieciowego z pakietu autonomicznego.

Zewnętrzne komputery stacjonarne są połączone z Serwerem administracyjnym.

Informacje o profilach połączenia dla użytkowników mobilnych

Mobilni użytkownicy laptopów (zwanych dalej również "urządzeniami") mogą potrzebować zmiany metody łączenia się z Serwerem administracyjnym lub przełączania pomiędzy Serwerami administracyjnymi w zależności od aktualnej lokalizacji urządzenia w sieci firmowej.

Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

Używanie różnych adresów jednego Serwera administracyjnego

Urządzenia z zainstalowanym Agentem sieciowym mogą łączyć się z Serwerem administracyjnym z poziomu wewnętrznej sieci organizacji lub Internetu. W tej sytuacji wymagane może być, aby Agent sieciowy używał innych adresów do łączenia się z Serwerem administracyjnym: zewnętrznego adresu Serwera administracyjnego dla połączenia internetowego oraz wewnętrznego adresu Serwera administracyjnego dla wewnętrznego połączenia sieciowego.

W tym celu musisz dodać profil (dla połączenia z Serwerem administracyjnym z poziomu internetu) do zasady Agenta sieciowego. Dodaj profil we właściwościach zasady (sekcja **Łączność**, podsekcja **Profile połączenia**). W oknie tworzenia profilu należy wyłączyć opcję **Użyj tylko do pobierania uaktualnień** oraz wybrać opcję **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu**. Jeśli do łączenia się z Serwerem administracyjnym używasz bramy połączenia (na przykład, w konfiguracji Kaspersky Security Center, opisanej w sekcji Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej), w odpowiednim polu profilu połączenia musisz określić adres bramy połączenia.

Przełączanie pomiędzy Serwerami administracyjnymi w zależności od aktualnej sieci

Jeśli organizacja posiada kilka biur z różnymi Serwerami administracyjnymi, a niektóre urządzenia z zainstalowanym Agentem sieciowym są przenoszone pomiędzy nimi, Agent sieciowy musi łączyć się z Serwerem administracyjnym sieci lokalnej w biurze, w którym znajduje się urządzenie.

W tej sytuacji konieczne jest utworzenie profilu dla połączenia z Serwerem administracyjnym we właściwościach zasady Agenta sieciowego dla każdego z biur, za wyjątkiem głównego biura, w którym znajduje się oryginalny macierzysty Serwer administracyjny. W profilach połączenia należy określić adresy Serwerów administracyjnych i włączyć lub wyłączyć opcję **Użyj tylko do pobierania uaktualnień**:

- Wybierz tę opcję, jeśli chcesz, aby Agent sieciowy zsynchronizował się z macierzystym Serwerem administracyjnym, a Serwer lokalny był używany tylko do pobierania uaktualnień.
- Wyłącz tę opcję, jeśli Agent sieciowy ma być całkowicie zarządzany przez lokalny Serwer administracyjny.

Następnie powinieneś ustalić warunki przełączania do nowo utworzonych profili: przynajmniej jeden warunek dla każdego z biur, za wyjątkiem głównego biura. Celem każdego warunku jest wykrycie elementów, które są specyficzne dla środowiska sieciowego w biurze. Jeśli warunek jest prawdziwy, odpowiedni profil zostaje aktywowany. Jeśli żaden z warunków nie jest prawdziwy, Agent sieciowy przełączy się do macierzystego Serwera administracyjnego.

Tworzenie profilu połączenia dla użytkowników mobilnych

Profil połączenia serwera administracyjnego jest dostępny tylko na urządzeniach działających pod kontrolą systemu Windows i macOS.

W celu utworzenia profilu połączenia Agenta sieciowego z Serwerem administracyjnym dla użytkowników mobilnych:

1. W drzewie konsoli wybierz grupę administracyjną zawierającą urządzenia klienckie, dla których chcesz utworzyć profil połączenia Agenta sieciowego z Serwerem administracyjnym.
2. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz utworzyć profil połączenia dla wszystkich urządzeń w grupie, w obszarze roboczym grupy, na zakładce **Zasady** wybierz zasadę Agenta sieciowego. Otwórz okno właściwości wybranej zasadę.
   - Jeśli chcesz utworzyć profil dla urządzenia w grupie, w obszarze roboczym grupy, na zakładce **Urządzenia** wybierz urządzenie i wykonaj następujące czynności:
     a. Otwórz okno właściwości wybranego urządzenia.
     b. W sekcji **Aplikacje** okna właściwości urządzenia wybierz Agenta sieciowego.
     c. Otwórz okno właściwości Agenta sieciowego.
3. W oknie właściwości, w sekcji **Łączność** wybierz podsekcję **Profile połączenia**.
4. W grupie ustawień **Profile połączeń Serwera administracyjnego** kliknij przycisk **Dodaj**.

   Domyślnie, lista profili połączeń zawiera profile <Tryb offline> i <Macierzysty serwer administracyjny>. Profili nie można modyfikować ani usunąć.

   Profil <Tryb offline> nie określa żadnego Serwera do nawiązania połączenia. Dlatego też, agent sieciowy, gdy zostaje przełączony do tego profilu, nie próbuje nawiązać połączenia z żadnym serwerem administracyjnym, gdy aplikacje zainstalowane na urządzeniach klienckich działają pod kontrolą zasad użytkownika mobilnego. Profil <Tryb offline> może być używany, jeśli urządzenia są odłączone od sieci.

Profil <Macierzysty serwer administracyjny> dotyczy połączenia z serwerem administracyjnym, który został wybrany podczas instalacji agenta sieciowego. Profil <Macierzysty serwer administracyjny> jest stosowany, gdy urządzenie jest ponownie podłączane do macierzystego Serwera administracyjnego po tym, jak przez jakiś czas działało w sieci zewnętrznej.

5. W otwartym oknie **Nowy profil** skonfiguruj profil połączenia:

   - **Nazwa profilu**

     W tym polu możesz przejrzeć lub zmienić nazwę profilu połączenia.

   - **Serwer administracyjny**

     Adres Serwera administracyjnego, z którym urządzenie klienckie musi łączyć się podczas aktywacji profilu.

   - **Port**

     Numer portu używanego do nawiązywania połączenia.

   - **Port SSL**

     Numer portu połączenia podczas używania portu SSL.

   - **Użyj SSL**

     Jeśli ta opcja jest włączona, połączenie jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

     Domyślnie opcja ta jest włączona. Zalecamy, aby nie wyłączać tej opcji, aby Twoje połączenie pozostało bezpieczne.

   - Kliknij odnośnik **Konfiguruj połączenie poprzez serwer proxy**, aby skonfigurować połączenie poprzez serwer proxy. Wybierz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest wybrana, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

     - **Adres serwera proxy**

       Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

     - **Numer portu**

       Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

     - **Uwierzytelnianie na serwerze proxy**

Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

- Nazwa użytkownika (to pole jest dostępne, jeśli opcja **Uwierzytelnianie na serwerze proxy** jest zaznaczona)

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

- Hasło (to pole jest dostępne, jeśli została wybrana opcja **Uwierzytelnianie na serwerze proxy**)

  Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

  Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

- Ustawienia bramy połączenia

  Adres bramy, poprzez którą urządzenia klienckie łączą się z Serwerem administracyjnym.

- Włącz tryb użytkownika mobilnego

  Jeśli ta opcja jest włączona, w przypadku połączenia przez ten profil, aplikacje zainstalowane na urządzeniu klienckim będą używać profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie opcja ta jest wyłączona.

- Użyj tylko do pobierania uaktualnień

  Jeżeli ta opcja jest włączona, profil będzie używany tylko do pobierania aktualizacji przez aplikacje zainstalowane na urządzeniu klienckim. Dla innych działań połączenie z Serwerem administracyjnym będzie nawiązywane z użyciem wstępnych ustawień określonych podczas instalacji Agenta sieciowego.

  Domyślnie opcja ta jest włączona.

- Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu

  Jeśli ta opcja jest włączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu ustawień określonych we właściwościach profilu.

  Jeśli ta opcja jest wyłączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu oryginalnych ustawień określonych podczas instalacji.

  Ta opcja jest dostępna, jeśli opcja **Użyj tylko do pobierania aktualizacji** jest wyłączona.

  Domyślnie opcja ta jest wyłączona.

6. Zaznacz opcję **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny**, aby zezwolić aplikacjom zainstalowanym na urządzeniu klienckim na korzystanie z profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego, za każdym razem, gdy Serwer administracyjny nie jest dostępny. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

Profil połączenia Agenta sieciowego z Serwerem administracyjnym zostanie utworzony dla użytkowników mobilnych. Jeśli agent sieciowy łączy się z serwerem administracyjnym przy użyciu tego profilu, aplikacje zainstalowane na urządzeniu klienckim będą używać zasad dla urządzeń w trybie użytkownika mobilnego lub zasad użytkownika mobilnego.

Informacje o przełączaniu Agenta sieciowego na inne Serwery administracyjne

Początkowe ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są definiowane podczas instalacji Agenta sieciowego. Aby przełączyć Agenta sieciowego na inne Serwery administracyjne, możesz użyć reguł przełączania. Ta funkcja jest obsługiwana tylko w przypadku agentów sieciowych zainstalowanych na urządzeniach z systemem Windows lub macOS.

Reguły przełączania mogą być uruchamiane przy zmianie następujących parametrów sieci:

- Domyślny adres bramy.
- Adres IP serwera protokołu dynamicznej konfiguracji hosta (DHCP).
- Sufiks DNS podsieci.
- Adres IP sieciowego serwera DNS.
- Dostępność domeny Windows. Ten parametr jest dostępny tylko dla urządzeń z systemem Windows.
- Adres podsieci i maska.
- Adres IP sieciowego serwera WINS. Ten parametr jest dostępny tylko dla urządzeń z systemem Windows.
- Nazwa DNS lub NetBIOS urządzenia klienckiego.
- Dostępność adresu połączenia SSL.

Jeśli reguły przełączania Agenta sieciowego na inne Serwery administracyjne zostały zmienione, Agent sieciowy odpowiada na zmiany w parametrach sieci w następujący sposób:

- Jeśli ustawienia sieci pokrywają się z ustawieniami jednej z utworzonych reguł, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym określonym w tej regule. Aplikacje zainstalowane na urządzeniach klienckich przełączają się do zasady użytkownika mobilnego pod warunkiem, że takie zachowanie jest dozwolone przez regułę.
- Jeśli nie jest stosowana żadna z reguł, Agent sieciowy przywróci ustawienia domyślne połączenia z Serwerem administracyjnym określone podczas instalacji. Aplikacje zainstalowane na urządzeniach klienckich przywracają aktywne profile.
- Jeśli Serwer administracyjny jest niedostępny, Agent sieciowy używa zasad użytkownika mobilnego.

Agent sieciowy przełącza się do zasady użytkownika mobilnego tylko wtedy, gdy opcja **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny** jest włączona w ustawieniach zasady Agenta sieciowego.

Ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są zapisywane w profilu połączenia. W profilu połączenia możesz utworzyć reguły przełączania urządzeń klienckich do zasad użytkownika mobilnego, a także skonfigurować profil tak, aby mógł być używany tylko do pobierania uaktualnień.

Tworzenie reguły przełączania Agenta sieciowego według lokalizacji sieciowej

Przełączanie agenta sieciowego według lokalizacji sieciowej jest dostępne tylko na urządzeniach działających pod kontrolą systemu Windows i macOS.

W celu utworzenia reguły przełączania Agenta sieciowego z jednego z Serwera administracyjnego na inny w przypadkui zmiany ustawień sieciowych:

1. W drzewie konsoli należy wybrać grupę administracyjną zawierającą urządzenia, dla których ma zostać utworzona reguła przełączania Agenta sieciowego według opisu lokalizacji sieciowej.
2. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz utworzyć regułę dla wszystkich urządzeń w grupie, w obszarze roboczym grupy, na zakładce **Zasady** wybierz zasadę Agenta sieciowego. Otwórz okno właściwości wybranej zasadę.
   - Jeśli chcesz utworzyć regułę dla urządzenia wybranego w grupie, w obszarze roboczym grupy, na zakładce **Urządzenia** wybierz urządzenie i wykonaj następujące czynności:
     a. Otwórz okno właściwości wybranego urządzenia.
     b. W sekcji **Aplikacje** okna właściwości urządzenia wybierz Agenta sieciowego.
     c. Otwórz okno właściwości Agenta sieciowego.
3. W otwartym oknie **właściwości**, w sekcji **Łączność** wybierz podsekcję **Profile połączenia**.
4. W sekcji **Ustawienia lokalizacji sieciowej** kliknij przycisk **Dodaj**.
5. W otwartym oknie **Nowy opis** skonfiguruj opis lokalizacji sieciowej i regułę przełączania. Określ następujące ustawienia opisu lokalizacji sieciowej:
   - Nazwa opisu lokalizacji sieciowej

     Nazwa opisu lokalizacji sieciowej nie może być dłuższa niż 255 znaków i nie może zawierać znaków specjalnych, takich jak ("*<>?\/:|).
   - Użyj profilu połączenia

Na liście rozwijalnej możesz określić profil połączenia, którego Agent sieciowy używa do nawiązania połączenia z Serwerem administracyjnym. Ten profil będzie używany, jeśli spełnione są warunki opisu lokalizacji sieciowej. Profil połączenia zawiera ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym i definiuje, kiedy urządzenia klienckie muszą przełączyć się do zasad użytkownika mobilnego. Profil jest używany tylko do pobierania uaktualnień.

6. W sekcji **Warunki przełączenia** kliknij przycisk **Dodaj**, aby utworzyć listę warunków opisu lokalizacji sieciowej.

   Warunki w regule są połączone przy użyciu operatora logicznego I. Aby wyzwolić regułę przełączania według opisu lokalizacji sieciowej, muszą być spełnione wszystkie warunki przełączania reguły.

7. Z listy rozwijalnej wybierz wartość odpowiadającą zmianie charakterystyki sieci, do której podłączone jest urządzenie klienckie:

   - **Adres domyślnej bramy połączenia** — zmiana adresu głównej bramy sieci.
   - **Adres serwera DHCP** — zmiana adresu IP serwera sieciowego (DHCP).
   - **Domena DNS** — zmiana sufiksu DNS podsieci.
   - **Adres serwera DNS** — zmiana adresu IP serwera DNS.
   - **Dostępność domeny Windows (tylko w systemie Windows)** – zmiana stanu domeny Windows, do której podłączone jest urządzenie klienckie. Użyj tego ustawienia tylko w przypadku urządzeń z systemem Windows.
   - **Podsieć** – zmiana adresu i maski podsieci.
   - **Adres serwera WINS (tylko w systemie Windows)** — adres IP sieciowego serwera WINS został zmieniony. Użyj tego ustawienia tylko w przypadku urządzeń z systemem Windows.
   - **Możliwość rozwiązywania nazw** — nazwa DNS lub NetBIOS urządzenia klienckiego uległa zmianie.
   - **Dostępność adresu połączenia SSL** — urządzenie klienckie może lub nie może (w zależności od wybranej opcji) nawiązać połączenie SSL z określonym Serwerem (nazwa:port). Dla każdego serwera możesz dodatkowo określić certyfikat SSL. W takim przypadku Agent sieciowy weryfikuje certyfikat Serwera, oprócz sprawdzenia możliwości połączenia SSL. Jeśli certyfikat nie pasuje, połączenie nie powiedzie się.

8. W otwartym oknie możesz określić warunek do przełączenia Agenta sieciowego do innego Serwera administracyjnego. Nazwa okna zależy od wartości wybranej w poprzednim kroku. Określ następujące ustawienia warunku przełączania:

   - Wartość

     W tym polu możesz dodać jeden lub kilka wartości dla tworzonego warunku.

   - Zgodny z przynajmniej jedną wartością z listy

     Jeśli ta opcja jest zaznaczona, warunek zostanie spełniony bez względu na wartość określoną na liście **Wartość**.

     Domyślnie opcja ta jest zaznaczona.

   - Niezgodny z żadną wartością z listy

Jeśli ta opcja jest zaznaczona, warunek zostanie spełniony, jeśli jego wartość nie znajduje się na liście **Wartość**.

9. W oknie **Nowy opis** zaznacz opcję **Opis włączony**, aby włączyć korzystanie z nowego opisu lokalizacji sieciowej.

Zostanie utworzona nowa reguła przełączania według opisu lokalizacji sieciowej. Za każdym razem, gdy zostaną spełnione warunki reguły, Agent sieciowy będzie używał profilu połączenia, określonego w regule, do łączenia się z Serwerem administracyjnym.

Opisy lokalizacji sieciowej są sprawdzane, czy pasują do układu sieci, zgodnie z ich kolejnością na liście. Jeżeli do sieci pasuje kilka opisów, użyty będzie pierwszy z nich. Możesz zmienić kolejność wyświetlania reguł na liście przy pomocy przycisków **W górę** (↑) i **W dół** (↓).

Szyfrowanie komunikacji z SSL/TLS

Aby usunąć luki w sieci korporacyjnej swojej organizacji, możesz włączyć szyfrowanie ruchu sieciowego przy użyciu SSL/TLS. Możesz włączyć SSL/TLS na Serwerze administracyjnym i Serwera iOS MDM. Kaspersky Security Center obsługuje SSL v3, a także Transport Layer Security (TLS v1.0, 1.1 i 1.2). Możesz wybrać protokół szyfrowania i zestawy szyfrowania. Kaspersky Security Center używa certyfikatów z podpisem własnym. Dodatkowa konfiguracja urządzeń iOS nie jest wymagana. Możesz także użyć swoich własnych certyfikatów. Specjaliści z Kaspersky zalecają używanie certyfikatów wydanych przez zaufane urzędy certyfikacji.

Serwer administracyjny

W celu skonfigurowania dozwolonych protokołów szyfrowania i zestawów szyfrowania na Serwerze administracyjnym:

1. Użyj narzędzia klscflag w celu skonfigurowania dozwolonych protokołów szyfrowania i zestawów szyfrowania na Serwerze administracyjnym. Wpisz następujące polecenie w wierszu poleceń systemu Windows, korzystając z uprawnień administratora:
   `klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <wartość> -t d`

   Określ parametr <wartość> polecenia:

   - `0`—wszystkie obsługiwane protokoły szyfrowania i zestawy szyfrowania są włączone
   - `1`—SSL v2 jest wyłączony

     Zestawy szyfrowania:

     - AES256-GCM-SHA384
     - AES256-SHA256
     - AES256-SHA
     - CAMELLIA256-SHA
     - AES128-GCM-SHA256

- AES128-SHA256
- AES128-SHA
- SEED-SHA
- CAMELLIA128-SHA
- IDEA-CBC-SHA
- RC4-SHA
- RC4-MD5
- DES-CBC3-SHA

- 2 — SSL v2 i SSL v3 są wyłączone (domyślna wartość)
  Zestawy szyfrowania:
  - AES256-GCM-SHA384
  - AES256-SHA256
  - AES256-SHA
  - CAMELLIA256-SHA
  - AES128-GCM-SHA256
  - AES128-SHA256
  - AES128-SHA
  - SEED-SHA
  - CAMELLIA128-SHA
  - IDEA-CBC-SHA
  - RC4-SHA
  - RC4-MD5
  - DES-CBC3-SHA
- 3 — tylko TLS v1.2.
  Zestawy szyfrowania:
  - AES256-GCM-SHA384
  - AES256-SHA256
  - AES256-SHA
  - CAMELLIA256-SHA

- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- CAMELLIA128-SHA

2. Uruchom ponownie następujące usługi Kaspersky Security Center 14.2:
   - Serwer administracyjny
   - Serwer sieciowy
   - Activation Proxy

Serwer iOS MDM

Połączenie między urządzeniami iOS a serwerem iOS MDM jest szyfrowane domyślnie.

W celu skonfigurowania dozwolonych protokołów szyfrowania i zestawów szyfrowania na serwerze iOS MDM:

1. Otwórz rejestr systemu urządzenia klienckiego, na którym jest zainstalowany serwer iOS MDM (na przykład, lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).
2. Przejdź do gałęzi:
   - W systemach 32-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - W systemach 64-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. Utwórz klucz o nazwie `StrictSslSettings`.
4. Jako typ klucza określ `DWORD`.
5. Określ wartość klucza:
   - `2`—SSL v3 jest wyłączony (TLS 1.0, TLS 1.1, TLS 1.2 są dozwolone)
   - `3`—tylko TLS 1.2 (domyślna wartość)
6. Uruchom ponownie usługę serwera iOS MDM Kaspersky Security Center.

Powiadomienia o zdarzeniach

Ta sekcja opisuje sposób wybrania metody dostarczenia administratorowi powiadomień o zdarzeniach, które wystąpiły na urządzeniach klienckich, a także sposób skonfigurowania ustawień powiadomień o zdarzeniach.

Znaleźć tu można także opis sposobu przetestowania dostarczania powiadomień o zdarzeniach przy użyciu wirusa testowego Eicar.

Konfigurowanie powiadomień o zdarzeniach

Kaspersky Security Center umożliwia wybranie metody powiadamiania administratora o zdarzeniach występujących na urządzeniach klienckich oraz skonfigurowanie powiadomień:

- Poprzez e-mail. Po wystąpieniu zdarzenia, aplikacja wyśle powiadomienie na określone adresy e-mail. Możesz zmodyfikować treść powiadomienia.
- Za pośrednictwem wiadomości SMS. Po wystąpieniu zdarzenia, aplikacja wyśle powiadomienie na określone numery telefonu. Możesz skonfigurować wysyłanie powiadomień SMS poprzez bramkę pocztową.
- Poprzez uruchomienie pliku wykonywalnego. Po wystąpieniu zdarzenia na urządzeniu, na stacji roboczej administratora zostanie uruchomiony plik wykonywalny. Korzystając z pliku wykonywalnego, administrator może pobrać parametry dowolnego zdarzenia, które wystąpiło.

W celu skonfigurowania wysyłania powiadomień o zdarzeniach występujących na urządzeniach klienckich:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Kliknij odnośnik **Konfiguruj powiadomienia i eksportowanie zdarzeń** i z listy rozwijalnej wybierz wartość **Konfiguruj powiadomienia**.

   Spowoduje to otwarcie okna **Właściwości: Zdarzenia**.
4. W sekcji **Powiadamianie** wybierz metodę powiadamiania (poprzez e-mail, za pośrednictwem wiadomości SMS lub przez uruchomienie pliku wykonywalnego) i zdefiniuj ustawienia powiadomień:

   - **E-mail**

Zakładka **E-mail** umożliwia skonfigurowanie wysyłania powiadomień o zdarzeniach za pośrednictwem poczty elektronicznej.

W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami.

W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX**, możesz użyć kilku wpisów MX adresów IP dla tej samej nazwy DNS serwera SMTP. Ta sama nazwa DNS może posiadać kilka wpisów MX z różnymi wartościami priorytetu odbierania wiadomości e-mail. Serwer administracyjny spróbuje wysłać powiadomienia e-mail do serwera SMTP w kolejności rosnącej priorytetów wpisów MX. Domyślnie opcja ta jest wyłączona.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX** i nie włączysz korzystania z ustawień TLS, zalecane jest użycie ustawień DNSSEC na urządzeniu serwerowym jako dodatkowego środka ochrony wysyłania powiadomień e-mail.

Kliknij odnośnik **Ustawienia**, aby zdefiniować dodatkowe ustawienia powiadomień:

- Nazwa podmiotu (nazwa podmiotu wiadomości e-mail)
- Adres e-mail nadawcy
- Ustawienia uwierzytelniania ESMTP

Jeśli dla serwera SMTP włączono uwierzytelnianie ESMTP, do autoryzacji na serwerze SMTP należy określić konto.

- Ustawienia TLS dla serwera SMTP:
  - **Nie korzystaj z TLS**

    Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.
  - **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

    Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.
  - **Zawsze używaj TLS, sprawdź certyfikat serwera pod kątem ważności**

    Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź certyfikat serwera pod kątem ważności**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić ustawienia TLS dla serwera SMTP:

- Odszukaj plik certyfikatu serwera SMTP:

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

- Odszukaj plik certyfikatu klienta:

Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

- Certyfikat X-509:

Musisz określić plik z certyfikatem oraz plik z kluczem prywatnym. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po załadowaniu obu plików należy określić hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- Kontener pkcs12:

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia. Lista dodatkowych parametrów jest dostępna po kliknięciu przycisku, znajdującego się z prawej strony pola.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%”.

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy poprawnie skonfigurowałeś powiadomienia. Aplikacja powinna wysłać powiadomienie testowe na adresy e-mail, które określiłeś.

- SMS

Na zakładce **SMS** możesz skonfigurować wysyłanie powiadomień SMS o różnych zdarzeniach na telefon komórkowy. Wiadomości SMS są wysyłane poprzez bramkę pocztową.

W polu **Odbiorcy (adresy e-mail)** określ adres e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami. Powiadomienia będą dostarczane na numery telefonów skojarzone z określonymi adresami e-mail.

W polu **Serwery SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Kliknij odnośnik **Ustawienia**, aby zdefiniować dodatkowe ustawienia powiadomień:

- Nazwa podmiotu (nazwa podmiotu wiadomości e-mail)
- Adres e-mail nadawcy
- Ustawienia uwierzytelniania ESMTP

Jeśli to konieczne, jeśli dla serwera SMTP włączono uwierzytelnianie ESMTP, do autoryzacji na serwerze SMTP możesz określić konto.

- Ustawienia TLS dla serwera SMTP

Możesz wyłączyć korzystanie z TLS, użyć TLS, jeśli serwer SMTP obsługuje ten protokół lub możesz wymusić użycie tylko TLS. Jeśli zdecydujesz się używać tylko TLS, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Dodatkowo, jeśli wybierzesz używanie tylko TLS, możesz określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

- Odszukaj plik certyfikatu serwera SMTP

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Kaspersky Security Center. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może zawierać pustą wartość, jeśli klucz prywatny nie zostanie zakodowane. Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami o zdarzeniu, które aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia. Lista dodatkowych parametrów jest dostępna po kliknięciu przycisku, znajdującego się z prawej strony pola.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%”.

Kliknij odnośnik **Ustaw limit liczby powiadomień**, aby określić maksymalną liczbę powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy powiadomienia zostały skonfigurowane poprawnie. Aplikacja powinna wysłać powiadomienie testowe do określonych odbiorców.

- Plik wykonywalny do uruchomienia

Jeśli wybrana jest ta metoda powiadamiania, w polu wejściowym określ aplikację, która zostanie uruchomiona, gdy wystąpi zdarzenie.

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Przycisk **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie na wskazany adres e-mail.

5. W polu **Treść powiadomienia** wprowadź tekst, który aplikacja wyśle po wystąpieniu zdarzenia.

   Możesz użyć listy rozwijanej znajdującej się na prawo od pola tekstowego, aby dodać dodatkowe ustawienia ze szczegółami zdarzenia (na przykład: opis zdarzenia lub czas wystąpienia).

   Jeżeli tekst powiadomienia zawiera znak %, należy go określić dwukrotnie, aby umożliwić wysłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%".

6. Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy powiadomienia zostały skonfigurowane poprawnie.

   Aplikacja wysyła powiadomienie testowe do określonego użytkownika.

7. Kliknij **OK**, aby zachować zmiany.

Skonfigurowane ustawienia powiadamiania zostaną zastosowane do wszystkich zdarzeń występujących na urządzeniach klienckich.

Możesz zastąpić ustawienia powiadamiania dla pewnych zdarzeń w sekcji **Konfiguracja zdarzenia** ustawień Serwera administracyjnego, ustawień profilu lub ustawień aplikacji.

Sprawdzanie opcji wysyłania powiadomień

Aby sprawdzić, czy powiadomienia o zdarzeniach są dostarczane, aplikacja używa powiadomień o wykryciu na urządzeniach klienckich „wirusa" testowego EICAR.

W celu sprawdzenia opcji wysyłania powiadomień o zdarzeniach:

1. Zatrzymaj zadanie ochrony systemu plików w czasie rzeczywistym na urządzeniu klienckim, a następnie skopiuj na nie „wirusa" testowego EICAR. Włącz ponownie ochronę w czasie rzeczywistym systemu plików.

2. Uruchom zadanie skanowania dla urządzeń klienckich w grupie administracyjnej lub dla wskazanych urządzeń, uwzględniając urządzenie zawierające „wirusa" testowego EICAR.

   Jeżeli zadanie skanowania jest skonfigurowane poprawnie, "wirus" testowy zostanie wykryty. Jeżeli powiadomienia są skonfigurowane poprawnie, zostaniesz powiadomiony o wykryciu wirusa.

   W obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Zdarzenia** wybór **Ostatnie zdarzenia** będzie wyświetlał wpis dotyczący wykrycia "wirusa".

EICAR nie zawiera kodu, który mógłby wyrządzić szkody na urządzeniu. Jednak większość aplikacji zabezpieczających wykrywa ten plik jako wirusa. „Wirusa" testowego możesz pobrać z oficjalnej strony EICAR.

Wyświetlanie powiadomień o zdarzeniach po uruchomieniu pliku wykonywalnego

Kaspersky Security Center może powiadamiać administratora o zdarzeniach na urządzeniach klienckich poprzez uruchomienie pliku wykonywalnego. Plik wykonywalny musi zawierać inny plik wykonywalny z symbolami zastępczymi zdarzenia przekazywanymi administratorowi.

Symbole zastępcze opisujące zdarzenie

Symbol zastępczy	Opis symbolu zastępczego
%SEVERITY%	Priorytet zdarzenia
%COMPUTER%	Nazwa urządzenia, na którym wystąpiło zdarzenie
%DOMAIN%	Domena
%EVENT%	Zdarzenie
%DESCR%	Opis zdarzenia
%RISE_TIME%	Czas wystąpienia zdarzenia
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nazwa zadania
%KL_PRODUCT%	Agent sieciowy Kaspersky Security Center
%KL_VERSION%	Numer wersji Agenta sieciowego
%HOST_IP%	Adres IP
%HOST_CONN_IP%	Adres IP połączenia.

Na przykład:
Powiadomienia o zdarzeniach są wysyłane przez plik wykonywalny (na przykład script1.bat), w którym uruchomiony jest inny plik wykonywalny (na przykład script2.bat) z symbolem zastępczym %COMPUTER%. Po wystąpieniu zdarzenia, plik script1.bat jest uruchamiany na urządzeniu administratora, który uruchamia plik script2.bat z symbolem zastępczym %COMPUTER%. Administrator uzyska nazwę urządzenia, na którym wystąpiło zdarzenie.

Konfigurowanie interfejsu

Możesz skonfigurować interfejs Kaspersky Security Center:

- Wyświetlić i ukryć obiekty w drzewie konsoli, w obszarze roboczym i w oknach właściwości obiektów (folderach, sekcjach) w zależności od funkcji, z której korzystasz.
- Wyświetlić i ukryć elementy okna głównego (na przykład drzewo konsoli lub standardowe menu, takie jak **Akcje** i **Widok**).

W celu skonfigurowania interfejsu Kaspersky Security Center zgodnie z aktualnie używanym zestawem funkcji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Na pasku menu okna głównego aplikacji wybierz **Widok** → **Konfiguruj interfejs**.

3. W oknie **Konfiguracja interfejsu**, które zostanie otwarte, skonfiguruj wyświetlanie elementów interfejsu, korzystając z następujących pól:

- **Wyświetl Zarządzanie lukami i poprawkami**

  Jeśli ta opcja jest włączona, w folderze **Zdalna instalacja** wyświetlany jest podfolder **Rozsyłanie obrazów urządzenia**, a w folderze **Repozytoria** wyświetlany jest podfolder **Sprzęt**.

  Ta opcja jest domyślnie wyłączona, jeśli działanie kreatora wstępnej konfiguracji nie zostało zakończone. Ta opcja jest domyślnie włączona, jeśli działanie kreatora wstępnej konfiguracji zostało zakończone.

- **Wyświetl szyfrowanie i ochronę danych**

  Jeśli ta opcja jest włączona, drzewo konsoli wyświetla folder **Szyfrowanie i ochrona danych**.

  Domyślnie opcja ta jest włączona.

- **Wyświetl ustawienia kontroli węzła końcowego**

  Jeśli ta opcja jest włączona, w sekcji **Kontrola zabezpieczeń** okna właściwości zasady Kaspersky Endpoint Security for Windows wyświetlane są następujące podsekcje:

  - **Kontrola aplikacji**
  - **Kontrola urządzeń**
  - **Kontrola sieci**
  - **Adaptacyjna kontrola nad anomaliami.**

  Jeśli ta opcja jest wyłączona, wyżej wymienione podsekcje nie są wyświetlane w sekcji **Kontrola zabezpieczeń**.

  Domyślnie opcja ta jest włączona.

- **Wyświetl Zarządzanie urządzeniami mobilnymi**

  Jeśli ta opcja jest włączona, funkcja **Zarządzanie urządzeniami mobilnymi** jest dostępna. Po ponownym uruchomieniu aplikacji, drzewo konsoli wyświetla folder **Urządzenia mobilne**.

  Domyślnie opcja ta jest włączona.

- **Wyświetl podrzędne Serwery administracyjne**

  Jeśli to pole jest zaznaczone, drzewo konsoli będzie wyświetlać węzły podrzędnych i wirtualnych Serwerów administracyjnych wchodzących w skład grup administracyjnych. Funkcje związane z podrzędnymi i wirtualnymi Serwerami administracyjnymi—na przykład, tworzenie zadań zdalnej instalacji aplikacji na podrzędnych Serwerach administracyjnych—będą dostępne.

  Domyślnie pole to nie jest zaznaczone.

- **Wyświetl sekcje ustawień zabezpieczeń**

Jeśli ta opcja jest włączona, sekcja **Zabezpieczenia** jest wyświetlana w oknie właściwości Serwera administracyjnego, grup administracyjnych i innych obiektów. Ta opcja umożliwia nadanie użytkownikom i grupom użytkowników niestandardowych uprawnień do pracy z obiektami.

Domyślnie opcja ta jest wyłączona.

4. Kliknij **OK**.

Aby zastosować niektóre zmiany, musisz zamknąć okno główne aplikacji, a następnie otworzyć je ponownie.

W celu skonfigurowania wyświetlania elementów w oknie głównym aplikacji:

1. Na pasku menu okna głównego aplikacji wybierz **Widok** → **Konfiguruj**.
2. W oknie **Konfiguracja widoku**, które zostanie otwarte, skonfiguruj wyświetlanie elementów okna głównego, korzystając z dostępnych pól.
3. Kliknij **OK**.

Wykrywanie urządzeń w sieci

Ta sekcja opisuje kroki, jakie musisz podjąć po zainstalowaniu Kaspersky Security Center.

Scenariusz: Wykrywanie urządzeń w sieci

Przed zainstalowaniem aplikacji zabezpieczających musisz przeprowadzić wykrywanie urządzeń. Serwer administracyjny otrzymuje informacje o wykrytych urządzeniach i umożliwia zarządzanie urządzeniami za pomocą profili. Do aktualizacji listy urządzeń dostępnych w sieci potrzebne są regularne ankiety sieciowe.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB1 jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Użyj następującego polecenia:
`Get-SmbServerConfiguration | select EnableSMB1Protocol`

Wykrywanie urządzeń sieciowych przebiega w następujących krokach:

1. **Odkryj urządzenia**

   Kreator wstępnej konfiguracji poprowadzi Cię przez wstępne wyszukiwanie urządzeń i pomoże w odnalezieniu urządzeń w sieci, takich jak komputery, tablety i telefony komórkowe. Możesz także ręcznie przeprowadzić wykrywanie urządzeń.

2. **Skonfiguruj zaplanowane ankiety**

   Zdecyduj, których typów przeszukiwania chcesz używać regularnie. Włącz żądane typy i skonfiguruj harmonogram ankiety według własnego uznania. Możesz zapoznać się z zaleceniami dotyczącymi częstotliwości odpytywania sieci.

3. **(Opcjonalnie) Skonfiguruj reguły dodawania wykrytych urządzeń do grup administracyjnych**

Jeśli nowe urządzenia pojawią się w Twojej sieci, zostaną wykryte podczas regularnych przeszukiwań i zostaną automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**. Możesz skonfigurować reguły przenoszenia urządzeń, aby zautomatyzować przydzielanie urządzeń do grupy **Zarządzane urządzenia**. Możesz także skonfigurować reguły zatrzymania.

Jeśli pominiesz krok 3, nowo wykryte urządzenia zostaną przydzielone do grupy **Urządzenia nieprzypisane**. Jeśli chcesz, możesz ręcznie przenieść te urządzenia do grupy **Zarządzane urządzenia**. Jeśli ręcznie przeniesiesz te urządzenia do grupy **Zarządzane urządzenia**, możesz przeanalizować informacje o każdym urządzeniu i zdecydować, czy chcesz przenieść je do grupy administracyjnej i do jakiej grupy.

Wyniki

Zakończenie scenariusza powoduje, że:

- Serwer administracyjny Kaspersky Security Center wykrywa urządzenia, które znajdują się w sieci, i zapewnia informacje o nich.
- Przyszłe przeszukiwania zostają skonfigurowane i przeprowadzone zgodnie z określonym terminarzem.
- Nowo wykryte urządzenia zostaną rozmieszczone zgodnie ze skonfigurowanymi regułami (lub jeśli nie ma skonfigurowanych reguł, urządzenia pozostają w grupie **Urządzenia nieprzypisane**).

Urządzenia nieprzypisane

Sekcja ta zawiera informacje o sposobie zarządzania urządzeniami w sieci firmowej, gdy nie należą do grupy administracyjnej.

Wykrywanie urządzeń

Ta sekcja opisuje typy wykrywania urządzeń dostępne w Kaspersky Security Center i oferuje informacje dotyczące korzystania z każdego typu.

Serwer administracyjny otrzymuje informacje o strukturze sieci i urządzeń w tej sieci poprzez regularne przeszukiwanie. Informacje są zapisywane w bazie danych Serwera administracyjnego. Serwer administracyjny może wykorzystywać następujące typy przeszukiwania:

- **Przeszukiwanie sieci Windows**. Serwer administracyjny może wykonywać dwa rodzaje przeszukiwań sieci Windows: szybkie i pełne. Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych. Podczas pełnego przeszukiwania wymaganych jest więcej informacji z urządzenia klienckiego, takich jak: nazwa systemu operacyjnego, adres IP, nazwa DNS, nazwa NetBIOS. Domyślnie włączone są oba przeszukiwania: szybkie i pełne. Przeszukiwanie sieci Windows może nie wykryć urządzeń, na przykład, jeśli porty UDP 137, UDP 138, TCP 139 są zamknięte na routerze lub przez zaporę sieciową.
- **Przeszukiwanie Active Directory**. Serwer administracyjny pobiera informacje na temat struktury jednostki Active Directory i nazw DNS urządzeń z grup Active Directory. Domyślnie ten typ przeszukiwania jest włączony. Zalecane jest użycie przeszukiwania Active Directory, jeśli używasz Active directory; w przeciwnym razie Serwer administracyjny nie wykryje żadnych urządzeń. Jeśli używasz Active Directory, ale niektóre z urządzeń w sieci nie są wymienione jako członkowie, te urządzenia nie mogą być wykrywane przez przeszukiwanie Active Directory.
- **Przeszukiwanie zakresu IP**. Serwer administracyjny przeszukuje określone zakresy IP przy użyciu pakietów ICMP lub protokołu NBNS i sporządza pełen zestaw danych na temat urządzeń znajdujących się w tych

zakresach IP. Domyślnie ten typ przeszukiwania jest wyłączony. Nie jest zalecane korzystanie z tego typu przeszukiwania, jeśli korzystasz z przeszukiwania sieci Windows i/lub przeszukiwania Active Directory.

- **Przeszukiwanie Zeroconf**. Punkt dystrybucji, który odpytuje sieć IPv6 za pomocą zero-configuration networking (zwany również *Zeroconf*). Domyślnie ten typ przeszukiwania jest wyłączony. Możesz użyć przeszukiwania Zeroconf, jeśli na punkcie dystrybucji działa system Linux.

Jeśli skonfigurowałeś i włączyłeś reguły przenoszenia urządzeń, nowo wykryte urządzenia są automatycznie umieszczane w grupie **Zarządzane urządzenia**. Jeśli nie włączono żadnych reguł przenoszenia, nowo wykryte urządzenia zostają automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**.

Możesz zmodyfikować ustawienia wykrywania urządzeń dla każdego typu. Na przykład, możesz chcieć zmodyfikować terminarz przeszukiwania lub ustawić, czy przeszukiwany ma być cały las Active Directory lub tylko określona domena.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB1 jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Użyj następującego polecenia:
`Get-SmbServerConfiguration | select EnableSMB1Protocol`

Przeszukiwanie sieci Windows

Informacje o przeszukiwaniu sieci Windows

Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych. Podczas pełnego przeszukiwania wymagane są następujące informacje o każdym urządzeniu klienckim:

- Nazwa systemu operacyjnego
- Adres IP
- Nazwa DNS
- Nazwa NetBIOS

Szybkie przeszukiwanie i pełne przeszukiwanie wymagają:

- Porty UDP 137/138, TCP 139, UDP 445, TCP 445 muszą być dostępne w sieci.
- Protokół SMB jest włączony.
- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na Serwerze administracyjnym.
- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na urządzeniach klienckich:
  - Przynajmniej na jednym urządzeniu, jeśli liczba urządzeń w sieci nie przekracza 32.
  - Przynajmniej na jednym urządzeniu dla każdego z 32 urządzeń w sieci.

Pełne przeszukiwanie może być uruchomione tylko wtedy, gdy szybkie przeszukiwanie było uruchomione przynajmniej raz.

Przeglądanie i modyfikowanie ustawień przeszukiwania sieci Windows

W celu zmodyfikowania ustawień dla przeszukiwania sieci Windows:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Domeny**.

   Do folderu **Urządzenia nieprzypisane** możesz przejść z folderu **Wykrywanie urządzeń**, klikając przycisk **Przeszukaj teraz**.

   W obszarze roboczym podfolderu **Domeny** zostanie wyświetlona lista urządzeń.

2. Kliknij **Przeszukaj teraz**.

   Zostanie otwarte okno właściwości domeny. Jeśli chcesz, zmodyfikuj ustawienia przeszukiwania sieci Windows:

   - **Włącz przeszukiwanie sieci Windows**

     Opcja ta jest wybrana domyślnie. Jeśli nie chcesz przeprowadzić przeszukiwania sieci Windows (na przykład, jeśli myślisz, że przeszukiwanie Active Directory wystarczy), możesz odznaczyć tę opcję.

   - **Ustaw terminarz szybkiego przeszukiwania**

Domyślnie czas ten wynosi 15 minut.

Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych.

Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

Dostępne są następujące opcje terminarza przeszukiwania:

- **Co N dni**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N minut**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

  Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

- **Według dni tygodnia**

  Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc, w określone dni wybranych tygodni**

  Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest włączona.

- **Ustaw terminarz pełnego przeszukiwania**

Domyślny przedział czasu wynosi jedną godzinę. Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

Dostępne są następujące opcje terminarza przeszukiwania:

- **Co N dni**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N minut**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

  Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

- **Według dni tygodnia**

  Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc, w określone dni wybranych tygodni**

  Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest włączona.

Jeśli chcesz przeprowadzić przeszukiwanie natychmiast, kliknij **Przeszukaj teraz**. Zostaną uruchomione oba typy przeszukiwań.

Na wirtualnym Serwerze administracyjnym ustawienia przeszukiwania sieci Windows można przeglądać i modyfikować w oknie ustawień punktu dystrybucji, w sekcji **Wykrywanie urządzeń**.

Przeszukiwanie Active Directory

Użyj przeszukiwania Active Directory, jeśli używasz Active Directory; w innym przypadku zalecane jest użycie innych typów przeszukiwania. Jeśli używasz Active Directory, ale niektóre z urządzeń w sieci nie są wymienione jako członkowie, te urządzenia nie mogą być wykrywane przez przeszukiwanie Active Directory.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB1 jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Użyj następującego polecenia: `Get-SmbServerConfiguration | select EnableSMB1Protocol`

Przeglądanie i modyfikowanie ustawień przeszukiwania Active Directory

W celu zmodyfikowania ustawień przeszukiwania grup Active Directory:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Active Directory**.

   Alternatywnie, z folderu **Urządzenia nieprzypisane** możesz przejść do folderu **Wykrywanie urządzeń**, klikając przycisk **Przeszukaj teraz**.

2. Kliknij **Konfiguruj przeszukiwanie**.

   Zostanie otwarte okno właściwości Active Directory. Jeśli chcesz, zmodyfikuj ustawienia przeszukiwania grupy Active Directory:

   - Włącz przeszukiwanie Active Directory

     Opcja ta jest wybrana domyślnie. Jednakże, jeśli nie używasz Active Directory, przeszukiwanie nie pobierze żadnych wyników. W tym przypadku możesz odznaczyć tę opcję.

   - Ustaw terminarz przeszukiwania

Domyślny przedział czasu wynosi jedną godzinę. Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

Dostępne są następujące opcje terminarza przeszukiwania:

- **Co N dni**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N minut**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

  Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

- **Według dni tygodnia**

  Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc, w określone dni wybranych tygodni**

  Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest włączona.

- **Zaawansowane**

Możesz wybrać, które domeny Active Directory przeszukiwać:

- Domena Active Directory, do której należy Kaspersky Security Center.
- Las domeny, do którego należy Kaspersky Security Center.
- Określona lista domen Active Directory.

  Jeśli wybierzesz tę opcję, możesz dodać domeny do obszaru przeszukiwania:

  - Kliknij przycisk **Dodaj**.
  - W odpowiednich polach określ adres kontrolera domeny, nazwę i hasło konta, aby uzyskać do niego dostęp.
  - Kliknij **OK**, aby zachować zmiany.

  Możesz wybrać adres kontrolera domeny na liście i kliknąć przyciski **Modyfikuj** lub **Usuń**, aby go zmodyfikować lub usunąć.
- Kliknij **OK**, aby zachować zmiany.

Jeśli chcesz przeprowadzić przeszukiwanie natychmiast, kliknij przycisk **Przeszukaj teraz**.

Na wirtualnym Serwerze administracyjnym ustawienia przeszukiwania grup Active Directory można przeglądać i modyfikować w oknie właściwości punktu dystrybucji, w sekcji **Wykrywanie urządzeń**.

Przeszukiwanie zakresu IP

Serwer administracyjny przeszukuje określone zakresy IP przy użyciu pakietów ICMP lub protokołu NBNS i sporządza pełen zestaw danych na temat urządzeń znajdujących się w tych zakresach IP. Domyślnie ten typ przeszukiwania jest wyłączony. Nie jest zalecane korzystanie z tego typu przeszukiwania, jeśli korzystasz z przeszukiwania sieci Windows i/lub przeszukiwania Active Directory.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB1 jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Użyj następującego polecenia:
`Get-SmbServerConfiguration | select EnableSMB1Protocol`

Przeglądanie i modyfikowanie ustawień przeszukiwania zakresu IP

W celu przejrzenia i zmodyfikowania ustawień przeszukiwania grup Zakres IP:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Zakresy IP**.

   Możesz przejść z folderu **Urządzenia nieprzypisane** do folderu **Wykrywanie urządzeń** poprzez kliknięcie **Przeszukaj teraz**.
2. Jeśli chcesz, w podfolderze **Zakresy IP** kliknij **Dodaj podsieć**, aby dodać zakres IP dla przeszukiwania, a następnie kliknij **OK**.
3. Kliknij **Konfiguruj przeszukiwanie**.

Zostanie otwarte okno właściwości zakresów IP. Jeśli chcesz, możesz zmodyfikować ustawienia przeszukiwania zakresu IP:

- **Włącz przeszukiwanie zakresu IP**

  Opcja ta nie jest wybrana domyślnie. Nie jest zalecane korzystanie z tego typu przeszukiwania, jeśli korzystasz z przeszukiwania sieci Windows i/lub przeszukiwania Active Directory.

- **Ustaw terminarz przeszukiwania**

  Domyślny czas to 420 minut. Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

  Dostępne są następujące opcje terminarza przeszukiwania:

  - **Co N dni**

    Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N minut**

    Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

    Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

  - **Według dni tygodnia**

    Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

    Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

  - **Co miesiąc, w określone dni wybranych tygodni**

    Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

    Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

  - **Uruchom pominięte zadania**

    Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

    Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

    Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

    Domyślnie opcja ta jest włączona.

Jeśli chcesz przeprowadzić przeszukiwanie natychmiast, kliknij **Przeszukaj teraz**. Ten przycisk jest dostępny tylko wtedy, gdy wybrałeś **Włącz przeszukiwanie zakresu IP**.

Na wirtualnym Serwerze administracyjnym ustawienia przeszukiwania zakresu IP można przeglądać i modyfikować w oknie właściwości punktu dystrybucji, w sekcji **Wykrywanie urządzeń**. Urządzenia klienckie wykryte podczas przeszukiwania zakresów IP są wyświetlane w folderze **Domeny** wirtualnego Serwera administracyjnego.

Przeszukiwanie Zeroconf

Ten typ przeszukiwania jest obsługiwany tylko w przypadku punktów dystrybucji opartych na systemie Linux.

Punkt dystrybucji może przeszukiwać sieci, które mają urządzenia z adresami IPv6. W takim przypadku zakresy adresów IP nie są określone, a punkt dystrybucji przeszukuje całą sieć za pomocą zero-configuration networking (zwany również *Zeroconf*). Aby rozpocząć korzystanie z Zeroconf, musisz zainstalować narzędzie avahi-browse w punkcie dystrybucji.

W celu włączenia przeszukiwania Zeroconf:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Zakresy IP**.

   Możesz przejść z folderu **Urządzenia nieprzypisane** do folderu **Wykrywanie urządzeń** poprzez kliknięcie **Przeszukaj teraz**.

2. Kliknij **Konfiguruj przeszukiwanie**.

3. W otwartym oknie właściwości zakresów adresów IP wybierz **Włącz przeszukiwanie za pomocą technologii Zeroconf**.

Następnie punkt dystrybucji zaczyna przeszukiwać sieć. W takim przypadku określone zakresy adresów IP są ignorowane.

Praca z domenami Windows. Przeglądanie i modyfikowanie ustawień domeny

W celu zmodyfikowania ustawień domeny:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Domeny**.

2. Wybierz domenę i otwórz okno jej właściwości w jeden z następujących sposobów:

   - z menu kontekstowego domeny wybierz polecenie **Właściwości**.
   - kliknij odnośnik **Pokaż właściwości grupy**.

   Zostanie otwarte okno **Właściwości: <Nazwa domeny>**, w którym możesz skonfigurować wybraną domenę.

Konfigurowanie reguły zatrzymania dla urządzeń nieprzypisanych

Po zakończeniu przeszukiwania sieci Windows, wykryte urządzenia zostały umieszczone w podgrupach grupy administracyjnej Urządzenia nieprzypisane. T grupę administracyjną można znaleźć w **Zaawansowane** → **Wykrywanie urządzeń** → **Domeny**. Folder **Domeny** to grupa nadrzędna. Zawiera grupy potomne, które zostały nazwane po odpowiednich domenach i grupach roboczych, które zostały wykryte podczas przeszukiwania sieci. Grupa nadrzędna może także zawierać grupę administracyjną urządzeń mobilnych. Możesz skonfigurować reguły zatrzymania urządzeń nieprzypisanych dla grupy nadrzędnej i dla każdej grupy potomnej. Reguły zatrzymania nie zależą od ustawień przeszukiwania sieci i działają nawet wtedy, gdy przeszukiwanie sieci jest wyłączone.

W celu skonfigurowania reguł zatrzymania dla urządzeń nieprzypisanych:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wykonaj jedną z następujących czynności:

   - Aby skonfigurować ustawienia grupy nadrzędnej, kliknij prawym klawiszem myszy podfolder **Domeny** i wybierz **Właściwości**.

     Zostanie otwarte okno właściwości grupy nadrzędnej.

   - Aby skonfigurować ustawienia grupy potomnej, kliknij jej nazwę prawym klawiszem myszy i z otwartego menu wybierz **Właściwości**.

     Zostanie otwarte okno właściwości grupy potomnej.

2. W sekcji **Urządzenia** określ następujące ustawienia:

   - **Usuń urządzenie z grupy, jeżeli było nieaktywne dłużej niż (dni)**

     Jeśli ta opcja jest włączona, możesz określić przedział czasu, po upływie którego urządzenie zostanie automatycznie usunięte z grupy. Domyślnie, ta opcja jest także rozsyłana do grup potomnych. Domyślny przedział czasu wynosi 7 dni.

     Domyślnie opcja ta jest włączona.

   - **Dziedzicz z grupy nadrzędnej**

     Jeśli ta opcja jest włączona, okres zatrzymania dla urządzeń w bieżącej grupie jest dziedziczony z grupy nadrzędnej nie może zostać zmieniony.

     Ta opcja jest dostępna tylko dla grup potomnych.

     Domyślnie opcja ta jest włączona.

   - **Wymuś dziedziczenie w grupach podrzędnych**

     Wartości ustawień zostaną rozesłane do grup potomnych, ale we właściwościach grup potomnych te ustawienia są zablokowane.

     Domyślnie opcja ta jest wyłączona.

Twoje zmiany zostaną zapisane i zastosowane.

Praca z zakresami IP

Możesz dostosować istniejące zakresy IP oraz utworzyć nowe.

Tworzenie zakresu IP

W celu utworzenia zakresu IP:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Zakresy IP**.
2. Z menu kontekstowego folderu wybierz **Nowy → Zakres IP**.
3. W oknie **Nowy zakres IP**, które zostanie otwarte, dostosuj ustawienia nowego zakresu IP.

Nowy zakres IP pojawi się w folderze **Zakresy IP**.

Przeglądanie i modyfikowanie ustawień zakresu IP

W celu zmodyfikowania ustawień zakresu IP:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Zakresy IP**.
2. Wybierz zakres IP i otwórz okno jego właściwości w jeden z następujących sposobów:
   - Z menu kontekstowego zakresu IP wybierz polecenie **Właściwości**.
   - kliknij odnośnik **Pokaż właściwości grupy**.

Zostanie otwarte okno **Właściwości: <Nazwa zakresu IP>**, w którym możesz skonfigurować właściwości wybranego zakresu IP.

Praca z grupami Active Directory. Przeglądanie i modyfikowanie ustawień grupy

W celu zmodyfikowania ustawień grupy Active Directory:

1. W drzewie konsoli, w folderze **Wykrywanie urządzeń** wybierz podfolder **Active Directory**.
2. Wybierz grupę Active Directory i otwórz okno jej właściwości w jeden z następujących sposobów:
   - Z menu kontekstowego zakresu IP wybierz polecenie **Właściwości**.
   - kliknij odnośnik **Pokaż właściwości grupy**.

Zostanie otwarte okno **Właściwości: <Nazwa grupy Active Directory>**, w którym można skonfigurować ustawienia wybranej grupy Active Directory.

Tworzenie reguł automatycznego przenoszenia urządzeń do grup administracyjnych

Możesz skonfigurować automatyczne przenoszenie urządzeń do grup administracyjnych po ich wykryciu podczas przeszukiwania sieci firmowej.

W celu skonfigurowania reguł automatycznego przenoszenia urządzeń do grup administracyjnych:

1. Z drzewa konsoli wybierz folder **Urządzenia nieprzypisane**.
2. W obszarze roboczym folderu kliknij **Konfiguruj reguły**.

   Spowoduje to otwarcie okna **Właściwości: Urządzenia nieprzypisane**. W sekcji **Przenieś urządzenia** skonfiguruj reguły automatycznego przenoszenia urządzeń do grup administracyjnych.

Do urządzenia zostanie zastosowana pierwsza odpowiednia reguła na liście (od góry do dołu listy).

Używanie dynamicznego trybu VDI na urządzeniach klienckich

Wirtualna infrastruktura może zostać wdrożona w sieci firmowej z użyciem tymczasowych maszyn wirtualnych. Kaspersky Security Center wykrywa tymczasowe maszyny wirtualne i dodaje o nich informacje do bazy danych Serwera administracyjnego. Gdy użytkownik zakończy korzystanie z tymczasowej maszyny wirtualnej, maszyna ta jest usuwana z wirtualnej infrastruktury. Wpis dotyczący usuniętej maszyny wirtualnej może być zapisany w bazie danych Serwera administracyjnego. Dodatkowo, w Konsoli administracyjnej mogą być wyświetlane nieistniejące maszyny wirtualne.

Aby informacje o nieistniejących maszynach wirtualnych nie były zapisywane, Kaspersky Security Center obsługuje tryb dynamiczny obsługi Virtual Desktop Infrastructure (VDI). Administrator może włączyć obsługę trybu dynamicznego dla VDI we właściwościach pakietu instalacyjnego Agenta sieciowego instalowanego na tymczasowej maszynie wirtualnej.

Jeśli tymczasowa maszyna wirtualna jest wyłączona, Agent sieciowy informuje Serwer administracyjny o jej wyłączeniu. Po pomyślnym wyłączeniu maszyny wirtualnej jest ona usuwana z listy urządzeń podłączonych do Serwera administracyjnego. Jeśli wyłączenie maszyny wirtualnej zakończyło się błędami, a Agent sieciowy nie wysłał do Serwera administracyjnego powiadomienia o wyłączonej maszynie wirtualnej, wdrażany jest scenariusz kopii zapasowej. W tym scenariuszu maszyna wirtualna jest usuwana z listy urządzeń podłączonych do Serwera administracyjnego po trzech niepomyślnych próbach synchronizacji z Serwerem administracyjnym.

Włączanie dynamicznego trybu VDI we właściwościach pakietu instalacyjnego Agenta sieciowego

W celu włączenia dynamicznego trybu VDI:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Z menu kontekstowego pakietu instalacyjnego Agenta sieciowego wybierz **Właściwości**.

   Zostanie otwarte okno **Właściwości: Agent sieciowy Kaspersky Security Center**.

3. W oknie **Właściwości: Agent sieciowy Kaspersky Security Center** wybierz sekcję **Zaawansowane**.
4. W sekcji **Zaawansowane** wybierz opcję **Włącz tryb dynamiczny VDI**.

Urządzenie, na którym jest instalowany Agent sieciowy, stanie się częścią VDI.

Wyszukiwanie urządzeń będących częścią VDI

W celu wyszukania urządzeń będących częścią VDI:

1. Wybierz **Szukaj** z menu kontekstowego folderu **Urządzenia nieprzypisane**.
2. W oknie **Wyszukaj urządzenia**, na zakładce **Maszyny wirtualne**, z listy rozwijalnej **Jest maszyną wirtualną** wybierz **Tak**.
3. Kliknij przycisk **Znajdź teraz**.

Aplikacja wyszuka urządzenia będące częścią infrastruktury Virtual Desktop Infrastructure.

Przenoszenie urządzeń z VDI do grupy administracyjnej

W celu przeniesienia urządzeń będących częścią VDI do grupy administracyjnej:

1. W obszarze roboczym folderu **Urządzenia nieprzypisane** kliknij **Konfiguruj reguły**.
   Zostanie otwarte okno właściwości folderu **Urządzenia nieprzypisane**.
2. W oknie właściwości folderu **Urządzenia nieprzypisane**, w sekcji **Przenieś urządzenia** kliknij przycisk **Dodaj**.
   Zostanie otwarte okno **Nowa reguła**.
3. W oknie **Nowa reguła** wybierz sekcję **Maszyny wirtualne**.
4. Z listy rozwijalnej **Jest maszyną wirtualną** wybierz **Tak**.

Zostanie utworzona reguła przeniesienia urządzenia do grupy administracyjnej.

Inwentaryzacja sprzętu

Lista sprzętu (**Repozytoria → Sprzęt**), której używasz do przeprowadzenia inwentaryzacji sprzętu, jest uzupełniana na dwa sposoby: automatycznie i ręcznie. Po każdym przeszukaniu sieci, wszystkie wykryte komputery zostają dodane do listy automatycznie; jednakże możesz także ręcznie dodać komputery, jeśli nie chcesz przeszukać sieci. Możesz ręcznie dodać inne urządzenia do listy, na przykład, routery, drukarki lub sprzęt komputerowy.

We właściwościach urządzenia możesz wyświetlić i zmodyfikować szczegółowe informacje o tym urządzeniu.

Lista sprzętu może zawierać następujące typy urządzeń:

- Komputery

- Urządzenia mobilne
- Urządzenia sieciowe
- Urządzenia wirtualne
- Składniki OEM
- Peryferia komputerowe
- Podłączone urządzenia
- Telefony VoIP
- Repozytoria sieciowe

Administrator może przypisać atrybut *Sprzęt firmowy* do wykrytych urządzeń. Ten atrybut jest przypisywany ręcznie we właściwościach urządzenia, administrator może również określić kryteria automatycznego przypisywania dla tego atrybutu. W takim przypadku atrybut *Sprzęt firmowy* jest przypisywany zgodnie z typem urządzenia.

Kaspersky Security Center pozwala na wyrejestrowywanie sprzętu. W tym celu wybierz opcję **Urządzenie wyrejestrowane** we właściwościach urządzenia. Takie urządzenie nie jest wyświetlane na liście sprzętu.

Administrator może zarządzać listą programowalnych sterowników logicznych (PLC) w folderze **Sprzęt**. Szczegółowe informacje na temat zarządzania listą PLC można znaleźć w *podręczniku użytkownika dla Kaspersky Industrial CyberSecurity for Nodes*.

Dodawanie informacji o nowych urządzeniach

W celu dodania informacji o nowych urządzeniach w sieci:

1. W folderze **Repozytoria** drzewa konsoli wybierz podfolder **Sprzęt**.
2. W obszarze roboczym folderu **Sprzęt** kliknij przycisk **Dodaj urządzenie**, aby otworzyć okno **Nowe urządzenie**.

   Zostanie otwarte okno **Nowe urządzenie**.
3. W oknie **Nowe urządzenie**, na liście rozwijalnej **Typ** wybierz typ urządzenia, które chcesz dodać.
4. Kliknij **OK**.

   Okno właściwości urządzenia zostanie otwarte na sekcji **Ogólny**.
5. W sekcji **Ogólny** wypełnij pola wejściowe danymi urządzenia. Sekcja **Ogólny** wyświetla następujące ustawienia:

   - **Urządzenie firmowe**. Zaznacz to pole, jeśli chcesz przypisać atrybut *Firmowy* do urządzenia. Przy użyciu tego atrybutu można wyszukiwać urządzenia w folderze **Sprzęt**.
   - **Urządzenie wyrejestrowane**. Zaznacz pole, jeśli nie chcesz, aby urządzenie było wyświetlane na liście urządzeń w folderze **Sprzęt**.
6. Kliknij **Zastosuj**.

Nowe urządzenie będzie wyświetlane w obszarze roboczym foldera **Sprzęt**.

Konfigurowanie kryteriów wykorzystywanych do określania urządzeń firmowych

W celu skonfigurowania kryteriów wykrywania dla urządzeń firmowych:

1. W folderze **Repozytoria** drzewa konsoli wybierz podfolder **Sprzęt**.
2. W obszarze roboczym folderu **Sprzęt** kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Ustaw regułę dla urządzeń firmowych**.

   Zostanie otwarte okno właściwości sprzętu.
3. W oknie właściwości sprzętu, w sekcji **Urządzenia firmowe** wybierz metodę przydzielania atrybutu *Firmowy* do urządzenia:

   - **Ustaw dla urządzenia atrybut urządzenie firmowe ręcznie**. Atrybut *Sprzęt firmowy* jest przypisywany do urządzenia ręcznie w oknie właściwości urządzenia, w sekcji **Ogólny**.
   - **Ustaw dla urządzenia atrybut urządzenie firmowego automatycznie**. W sekcji ustawień **Według typu urządzenia** określ typy urządzeń, dla których aplikacja będzie automatycznie przydzielać atrybut *Firmowy*.

     Ta opcja dotyczy tylko urządzeń, które zostały dodane przez przeszukiwanie sieci. W przypadku urządzeń dodanych ręcznie ustaw atrybut *Firmowy* ręcznie.
4. Kliknij **OK**.

Skonfigurowano kryteria wykrywania dla urządzeń firmowych.

Konfiguracja pól niestandardowych

W celu skonfigurowania niestandardowych pól urządzeń:

1. W folderze **Repozytoria** drzewa konsoli wybierz podfolder **Sprzęt**.
2. W obszarze roboczym folderu **Sprzęt** kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Konfiguruj niestandardowe pola danych**.

   Zostanie otwarte okno właściwości sprzętu.
3. W oknie właściwości sprzętu wybierz sekcję **Pola niestandardowe** i kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj pole**.
4. W oknie **Dodaj pole** określ nazwę pola niestandardowego, które będzie wyświetlane we właściwościach sprzętu.

   Możesz utworzyć kilka pól niestandardowych z unikatowymi nazwami.
5. Kliknij **OK**.

Dodane pola niestandardowe są wyświetlane w sekcji **Pola niestandardowe** właściwości sprzętu. Możesz użyć pół niestandardowych do dostarczenia określonych informacji o urządzeniach. Na przykład, to może być wewnętrzny numer zamówienia dla zakupu sprzętu.

Licencjonowanie

Ta sekcja zawiera informacje dotyczące ogólnych zasad związanych z licencjonowaniem Kaspersky Security Center 14.2.

Zdarzenia przekroczenia ograniczeń licencyjnych

Kaspersky Security Center pozwala uzyskać informacje o zdarzeniach, gdy pewne ograniczenia licencyjne zostaną przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich.

Priorytet takich zdarzeń, gdy ograniczenia licencyjne zostaną przekroczone, jest definiowany zgodnie z następującymi regułami:

- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją mieści się w 90% do 100% całkowitej liczby jednostek objętych licencją, publikowane zdarzenie posiada poziom istotności **Informacja**.
- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją mieści się w 100% do 110% całkowitej liczby jednostek objętych licencją, publikowane zdarzenie posiada poziom istotności **Ostrzeżenie**.
- Jeśli liczba aktualnie używanych jednostek objętych jedną licencją przekracza 110% całkowitej liczby jednostek objętych licencją, publikowane zdarzenie posiada poziom istotności **Zdarzenie krytyczne**.

Informacje o licencjonowaniu

Ta sekcja zawiera informacje o licencjonowaniu aplikacji firmy Kaspersky zarządzanej za pośrednictwem Kaspersky Security Center.

Informacje o licencji

Licencja to czasowo ograniczone prawo do korzystania z aplikacji nadane zgodnie z warunkami Umowy licencyjnej.

Licencja upoważnia do korzystania z następujących usług:

- Korzystania z aplikacji zgodnie z warunkami Umowy licencyjnej
- Uzyskania pomocy technicznej

Zakres świadczonych usług oraz okres ważności zależą od typu licencji użytej do aktywacji aplikacji.

Dostępne są następujące typy licencji:

- *Test.* Darmowa licencja udostępniana w celu zapoznania się z aplikacją.

  Licencja testowa ma zazwyczaj krótki okres ważności. Jeśli licencja testowa wygaśnie, wszystkie funkcje Kaspersky Security Center zostają wyłączone. Aby kontynuować korzystanie z aplikacji, należy zakupić licencję komercyjną.

  Możesz aktywować aplikację licencją testową tylko raz.

- *Reklama w telewizji.* Płatna licencja oferowana podczas zakupu aplikacji.

  Po wygaśnięciu licencji komercyjnej kluczowe funkcje aplikacji zostają wyłączone. Aby kontynuować korzystanie z Kaspersky Security Center, musisz odnowić swoją licencję komercyjną. Jeśli nie planujesz odnawiać licencji, musisz usunąć aplikację ze swojego komputera.

Zalecamy odnowienie licencji przed jej wygaśnięciem, aby zapewnić maksymalną ochronę przed wszystkimi zagrożeniami.

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 uważnie przeczytaj Umowę licencyjną.

Program Kaspersky Security Center i jego komponenty, na przykład, Agent sieciowy, ma swoją własną Umowę licencyjną.

Z warunkami Umowy licencyjnej dla Kaspersky Security Center można zapoznać się, korzystając z następujących metod:

- Podczas instalacji Kaspersky Security Center.
- W dokumencie license.txt, znajdującym się w pakiecie dystrybucyjnym Kaspersky Security Center.
- W dokumencie license.txt, znajdującym się w folderze instalacyjnym Kaspersky Security Center.
- Pobierając plik license.txt ze strony Kaspersky.

Warunki Umowy licencyjnej dla Agenta sieciowego dla systemu Windows, Agenta sieciowego dla systemu Mac, Agenta sieciowego dla systemu Linux można przejrzeć przy użyciu następujących metod:

- Podczas pobierania pakietu dystrybucyjnego Agenta sieciowego z serwerów sieciowych Kaspersky.
- Podczas instalacji Agenta sieciowego dla systemu Windows, Agenta sieciowego dla systemu Mac, Agenta sieciowego dla systemu Linux.
- Otwierając dokument license.txt znajdujący się w pakiecie dystrybucyjnym Agenta sieciowego dla systemu Windows, Agenta sieciowego dla systemu Mac, Agenta sieciowego dla systemu Linux.
- Otwierając dokument license.txt znajdujący się w folderze instalacyjnym Agenta sieciowego dla systemu Windows, Agenta sieciowego dla systemu Mac, Agenta sieciowego dla systemu Linux.
- Pobierając plik license.txt ze strony Kaspersky.

Akceptujesz warunki Umowy licencyjnej, zaznaczając odpowiednią opcję podczas instalacji aplikacji. Jeśli nie akceptujesz warunków Umowy licencyjnej, anuluj instalację aplikacji i nie używaj aplikacji.

Informacje o certyfikacie licencji

Certyfikat licencji to dokument, który otrzymujesz wraz z plikiem klucza lub kodem aktywacyjnym.

Certyfikat licencji zawiera następujące informacje o dostarczonej licencji:

- Klucz licencyjny lub numer zamówienia
- Informacje o użytkowniku, który otrzymał licencję
- Informacje o aplikacji, która może być aktywowana za pomocą zakupionej licencji
- Ograniczenie liczby urządzeń objętych zakupioną licencją
- Data rozpoczęcia okresu ważności licencji
- Data wygaśnięcia licencji lub okres ważności licencji
- Typ licencji

Informacje o kluczu licencyjnym

Klucz licencyjny jest to sekwencja bitów, które możesz zastosować w celu aktywacji, a następnie użyć aplikacji zgodnie z warunkami Umowy licencyjnej. Klucze licencyjne są generowane przez specjalistów z Kaspersky.

Możesz dodać klucz licencyjny do aplikacji, korzystając z następujących metod: stosując *plik klucza* lub wprowadzając *kod aktywacyjny*. Po dodaniu klucza licencyjnego do aplikacji jest on wyświetlany w interfejsie aplikacji jako unikatowa sekwencja alfanumeryczna.

Klucz licencyjny może zostać zablokowany przez Kaspersky w przypadku naruszenia warunków Umowy licencyjnej. Jeśli klucz licencyjny został zablokowany, aby móc korzystać z aplikacji, musisz dodać inny klucz.

Klucz licencyjny musi być aktywny lub dodatkowy (lub zapasowy).

Aktywny klucz licencyjny to klucz licencyjny, który jest aktualnie używany przez aplikację. Aktywny klucz licencyjny może zostać dodany dla licencji testowej lub komercyjnej. Aplikacja nie może posiadać więcej niż jednego aktywnego klucza licencyjnego.

Dodatkowy (lub zapasowy) klucz licencyjny to klucz licencyjny, który upoważnia użytkownika do korzystania z aplikacji, ale nie jest aktualnie w użyciu. Dodatkowy klucz licencyjny staje się aktywny automatycznie po wygaśnięciu licencji skojarzonej z bieżącym aktywnym kluczem licencyjnym. Dodatkowy klucz licencyjny może zostać dodany tylko wtedy, gdy aktywny klucz licencyjny został już dodany.

Klucz licencyjny dla licencji testowej można dodać tylko jako aktywny klucz licencyjny. Klucz licencyjny dla licencji testowej nie może zostać dodany jako dodatkowy klucz licencyjny.

Informacje o pliku klucza

Plik klucza to plik z rozszerzeniem .key, dostarczony przez firmę Kaspersky. Pliki kluczy zostały zaprojektowane do aktywowania aplikacji poprzez dodanie klucza licencyjnego.

Plik klucza otrzymasz na adres e-mail, który określiłeś podczas zakupu Kaspersky Security Center lub po zamówieniu wersji testowej Kaspersky Security Center.

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

W sytuacji przypadkowego usunięcia pliku klucza istnieje możliwość jego odzyskania. Plik klucza może być niezbędny, na przykład, do zarejestrowania konta Kaspersky CompanyAccount.

W celu odzyskania pliku klucza, należy wykonać jedną z poniższych czynności:

- Skontaktuj się ze sprzedawcą licencji.
- Uzyskaj plik klucza poprzez stronę internetową Kaspersky, korzystając z dostępnego kodu aktywacyjnego.

Informacje o subskrypcji

Subskrypcja na Kaspersky Security Center jest to zamówienie aplikacji z wybranymi ustawieniami (data wygaśnięcia subskrypcji, liczba chronionych urządzeń). Możesz zarejestrować swoją subskrypcję na Kaspersky Security Center u swojego dostawcy usługi (na przykład, dostawcy internetu). Subskrypcja może być odnawiana ręcznie lub automatycznie. Istnieje również możliwość jej anulowania.

Subskrypcja może być ograniczona (na przykład, na jeden rok) lub nieograniczona (bez daty wygaśnięcia). Aby możliwe było kontynuowanie korzystania z Kaspersky Security Center po wygaśnięciu ograniczonej subskrypcji, należy ją odnowić. Nieograniczona subskrypcja jest odnawiana automatycznie, jeśli została opłacona w odpowiednim terminie.

Po wygaśnięciu ograniczonej subskrypcji, może zostać zaoferowany okres karencji na odnowienie subskrypcji, w trakcie którego aplikacja będzie dalej działała. Dostępność i czas trwania okresu karencji są definiowane przez dostawcę usługi.

Aby używać Kaspersky Security Center z subskrypcją, należy wprowadzić kod aktywacyjny otrzymany od dostawcy usługi.

Możesz zastosować dla Kaspersky Security Center inny kod aktywacyjny dopiero wtedy, gdy Twoja subskrypcja wygaśnie lub gdy ją anulujesz.

W zależności od dostawcy usługi, zestaw możliwych działań do zarządzania subskrypcją może się różnić. Dostawca usługi może nie zaoferować okresu karencji na odnowienie subskrypcji i wówczas aplikacja przestanie działać.

Kody aktywacyjne zakupione dla subskrypcji nie mogą zostać użyte do aktywowania wcześniejszych wersji Kaspersky Security Center.

Jeśli korzystasz z aplikacji z subskrypcją, Kaspersky Security Center automatycznie próbuje uzyskać dostęp do serwera aktywacji w określonych przedziałach czasu, aż do wygaśnięcia subskrypcji. Jeżeli dostęp do serwera za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Możesz odnowić swoją subskrypcję na stronie dostawcy usługi.

Informacje o kodzie aktywacyjnym

Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Możesz wprowadzić kod aktywacyjny w celu dodania klucza licencyjnego aktywującego Kaspersky Security Center. Kod aktywacyjny otrzymasz na adres e-mail, który określiłeś podczas składania zamówienia, po zakupieniu Kaspersky Security Center lub po zamówieniu wersji testowej Kaspersky Security Center.

Aby aktywować aplikację kodem aktywacyjnym, potrzebny jest dostęp do internetu w celu nawiązania połączenia z serwerami aktywacji Kaspersky. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Jeśli aplikacja była aktywowana przy użyciu kodu aktywacyjnego, w niektórych przypadkach aplikacja wysyła regularne żądania do serwerów aktywacji Kaspersky w celu sprawdzenia bieżącego stanu klucza licencyjnego. Aby możliwe było wysyłanie żądań, należy zapewnić aplikacji dostęp do internetu.

Jeśli zgubiłeś kod aktywacyjny po zainstalowaniu aplikacji, skontaktuj się z partnerem Kaspersky, od którego zakupiłeś licencję.

Nie można używać plików kluczy do aktywacji zarządzanych aplikacji; akceptowane są tylko kody aktywacyjne.

Wycofanie zgody z Umową Licencyjną Użytkownika Końcowego

Jeśli decydujesz się zatrzymać ochronę swoich urządzeń klienckich, możesz odinstalować zarządzane aplikacje firmy Kaspersky i anulować swoją Umowę licencyjną dla tych aplikacji.

W celu anulowania Umowy licencyjnej dla zarządzanych aplikacji Kaspersky:

1. W drzewie konsoli wybierz **Serwer administracyjny** → **Zaawansowane** → **Zaakceptowane Umowy licencyjne**.

   Wyświetlana jest lista Umów licencyjnych, zaakceptowanych po utworzeniu pakietów instalacyjnych, w momencie bezproblemowej instalacji aktualizacji lub po zdalnym zainstalowaniu Kaspersky Security for Mobile.

2. Z listy wybierz Umowę licencyjną, którą chcesz anulować.

   Możesz sprawdzić następujące właściwości Umowy licencyjnej:

   - Datę zaakceptowania Umowy licencyjnej.
   - Nazwę użytkownika, który zaakceptował Umowę licencyjną.
   - Odnośnik do warunków Umowy licencyjnej.
   - Listy obiektów, które są powiązane z Umową licencyjną: nazwy pakietów instalacyjnych, nazwy aktualizacji typu seamless, nazwy aplikacji mobilnych.

3. Kliknij przycisk **Wycofaj Umowę licencyjną**.

   W otwartym oknie zostanie wyświetlona informacja, że musisz odinstalować aplikację firmy Kaspersky odpowiadającą Umowie licencyjnej.

4. Kliknij przycisk, aby potwierdzić wycofanie.

   Kaspersky Security Center sprawdzi, czy pakiety instalacyjne (odpowiadające zarządzanej aplikacji firmy Kaspersky, której Umowę licencyjną chcesz anulować) są odinstalowane.

   Możesz anulować tylko Umowę licencyjną dla zarządzanej aplikacji firmy Kaspersky, której pakiety instalacyjne są usuwane.

Umowa licencyjna zostanie wycofana. Nie jest wyświetlana na liście Umów licencyjnych w sekcji **Serwer administracyjny → Zaawansowane → Zaakceptowane Umowy licencyjne**. Nie możesz chronić urządzeń klienckich przy pomocy aplikacji firmy Kaspersky, której Umowę licencyjną wycofałeś.

Informacje o przekazywaniu danych

Dane przesyłane do firm trzecich

Jeśli korzystasz z funkcji zarządzania urządzeniami mobilnymi Oprogramowania, do czasowego dostarczenia poleceń na urządzenia działające pod kontrolą systemu operacyjnego Android poprzez mechanizm powiadomień push używana jest usługa Google Firebase Cloud Messaging. Jeśli Użytkownik skonfigurował użycie usługi Google Firebase Cloud Messaging, Użytkownik akceptuje dostarczenie następujących informacji do usługi Google Firebase Cloud Messaging w trybie automatycznym: identyfikator instalacji aplikacji Kaspersky Endpoint Security for Android, do której musi zostać wysłane powiadomienie push.

Aby zapobiec wymianie informacji z usługą Google Firebase Cloud Messaging, Użytkownik musi wycofać ustawienia korzystania z usługi Google Firebase Cloud Messaging do wartości fabrycznych.

Jeśli korzystasz z funkcji zarządzania urządzeniami mobilnymi Oprogramowania, do czasowego dostarczenia poleceń na urządzenia działające pod kontrolą systemu operacyjnego iOS poprzez mechanizm powiadomień push używana jest usługa Apple Push Notification Service (APNs). Jeśli Użytkownik zainstalował certyfikat APNs na serwerze iOS MDM, utworzył profil iOS MDM ze zbiorem ustawień do podłączenia urządzeń mobilnych iOS z Oprogramowaniem i zainstalował ten profil na urządzeniach mobilnych, Użytkownik wyraża zgodę na dostarczenie następujących informacji do APNs w trybie automatycznym:

- Token—push token urządzenia. Serwer używa tego tokena podczas wysyłania powiadomień push do urządzenia.
- PushMagic—ciąg znaków, który musi zostać zawarty w powiadomieniu push. Ta wartość ciągu znaków jest generowana przez urządzenie.

Dane przetwarzane lokalnie

Kaspersky Security Center służy do scentralizowanego wykonywania podstawowych zadań dotyczących administracji i zarządzania w sieci firmy. Kaspersky Security Center zapewnia administratorowi dostęp do szczegółowych informacji dotyczących poziomu ochrony sieci organizacji; Kaspersky Security Center umożliwia administratorowi skonfigurowanie wszystkich składników ochrony opartych o aplikacje Kaspersky. Kaspersky Security Center wykonuje następujące główne funkcje:

- Wykrywanie urządzeń i ich użytkowników w sieci organizacji
- Tworzenie hierarchii grup administracyjnych dla zarządzania urządzeniem
- Instalowanie aplikacji firmy Kaspersky na urządzeniach
- Zarządzanie ustawieniami i zadaniami zainstalowanych aplikacji
- Zarządzanie aktualizacjami dla aplikacji firmy Kaspersky oraz aplikacji firm trzecich, a także wyszukiwanie i eliminowanie luk
- Aktywowanie aplikacji firmy Kaspersky na urządzeniach
- Zarządzanie kontami użytkowników

- Przeglądanie informacji o działaniu aplikacji firmy Kaspersky na urządzeniach
- Przeglądanie raportów

Aby program Kaspersky Security Center mógł wykonywać główne funkcje, może otrzymywać, przechowywać i przetwarzać następujące informacje:

- Informacje o urządzeniach w sieci organizacji otrzymane w wyniku wykrywania urządzeń w sieci Active Directory lub sieci Windows lub poprzez skanowanie interwałów IP. Serwer administracyjny gromadzi dane niezależnie lub pobiera dane z Agenta sieciowego.
- Informacje o jednostkach organizacyjnych, domenach, użytkownikach i grupach Active Directory otrzymanych w wyniku wykrywania urządzeń w sieci Active Directory. Serwer administracyjny gromadzi dane niezależnie lub pobiera dane z Agenta sieciowego.
- Szczegóły dotyczące zarządzanych urządzeń. Agent sieciowy przesyła dane wymienione poniżej z urządzenia na Serwer administracyjny. Użytkownik wprowadza wyświetlaną nazwę oraz opis urządzenia w interfejsie Konsoli administracyjnej lub w interfejsie Kaspersky Security Center Web Console:
  - Specyfikacje techniczne zarządzanego urządzenia i jego komponenty wymagane do identyfikacji urządzenia: wyświetlana nazwa i opis urządzenia, typ i nazwa domeny Windows, nazwa urządzenia w środowisku Windows, domena DNS i nazwa DNS, adres IPv4, adres IPv6, lokalizacja sieci, adres MAC, typ systemu operacyjnego, czy urządzenie to maszyna wirtualna wraz z typem hipernadzorcy oraz czy urządzenie jest dynamiczną maszyną wirtualną jako część VDI.
  - Inne specyfikacje zarządzanych urządzeń i ich komponenty wymagane do audytu zarządzanych urządzeń oraz do podejmowania decyzji odnośnie tego, czy określone poprawki i aktualizacje są stosowane: stan Agenta Windows Update (WUA), architektura systemu operacyjnego, producent systemu operacyjnego, numer kompilacji systemu operacyjnego, identyfikator publikacji systemu operacyjnego, folder lokalizacyjny, jeśli urządzenie jest maszyną wirtualną—typ maszyny wirtualnej; nazwa wirtualnego Serwera administracyjnego, który zarządza urządzeniem; dane urządzenia w chmurze (region w chmurze, VPC, strefa dostępności w chmurze, podsieć w chmurze, strefa umieszczenia w chmurze).
  - Szczegóły dotyczące działań na zarządzanych urządzeniach: data i godzina ostatniej lokalizacji, czas, gdy urządzenie było ostatnio widoczne w sieci, stan oczekiwania na ponowne uruchomienie oraz czas, gdy urządzenie było włączone.
  - Szczegóły kont użytkownika na urządzeniu i sesji ich pracy.
- Statystyki działania punktu dystrybucji, jeśli urządzenie jest punktem dystrybucji. Agent sieciowy przesyła dane z urządzenia na Serwer administracyjny.
- Ustawienia punktu dystrybucji wprowadzone przez Użytkownika w Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console.
- Dane niezbędne do nawiązania połączenia między urządzeniami mobilnymi a Serwerem administracyjnym: certyfikat, port połączenia urządzenia mobilnego, adres połączenia Serwera administracyjnego. Użytkownik wprowadza dane w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
- Szczegóły urządzeń mobilnych przesyłane przy użyciu protokołu Exchange ActiveSync. Dane wymienione poniżej są przesyłane z urządzenia mobilnego na Serwer administracyjny:
  - Specyfikacje techniczne urządzenia mobilnego i jego komponentów wymagane do identyfikacji urządzenia: nazwa urządzenia, model, nazwa systemu operacyjnego, numer IMEI i numer telefonu.
  - Specyfikacje urządzenia mobilnego i jego komponentów: stan zarządzania urządzeniem, obsługa wiadomości SMS, uprawnienie do wysyłania wiadomości SMS, obsługa FCM, obsługa poleceń użytkownika, folder przechowywania systemu operacyjnego i nazwa urządzenia.

- Szczegóły działań na urządzeniach mobilnych: lokalizacja urządzenia (za pomocą polecenia Zlokalizuj), czas ostatniej synchronizacji, czas ostatniego połączenia z Serwerem administracyjnym, a także szczegóły obsługi synchronizacji.

- Szczegóły urządzeń mobilnych przesyłane przy użyciu protokołu iOS MDM. Dane wymienione poniżej są przesyłane z urządzenia mobilnego na Serwer administracyjny:

  - Specyfikacje techniczne urządzenia mobilnego i jego składników wymagane do identyfikacji urządzenia: nazwa urządzenia, model, nazwa systemu operacyjnego, numer kompilacji systemu operacyjnego, numer modelu urządzenia, numer IMEI, UDID, MEID, numer seryjny, ilość pamięci, wersja oprogramowania firmware modemu, adres MAC Bluetooth, adres MAC Wi-Fi i szczegóły karty SIM (identyfikator ICCID jako część identyfikatora karty SIM).

  - Szczegóły dotyczące sieci komórkowej używanej przez zarządzane urządzenie: typ sieci komórkowej, nazwa aktualnie używanej sieci komórkowej, nazwa domowej sieci komórkowej, wersja ustawień operatora sieci mobilnej, stan roamingu połączeń głosowych i stan roamingu danych, kod kraju sieci domowej, kod kraju zamieszkania, kod kraju aktualnie używanej sieci i poziom szyfrowania.

  - Ustawienia zabezpieczeń urządzenia mobilnego: użycie hasła i jego zgodność z ustawieniami zasady, lista profili konfiguracyjnych i profili informacyjnych używanych do zainstalowania aplikacji firm trzecich.

  - Data ostatniej synchronizacji z Serwerem administracyjnym i stan zarządzania urządzeniem.

- Szczegóły aplikacji Kaspersky zainstalowanych na urządzeniu. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego:

  - Ustawienia aplikacji firmy Kaspersky zainstalowanych na zarządzanym urządzeniu: nazwa i wersja aplikacji firmy Kaspersky, stan ochrony w czasie rzeczywistym, data i godzina ostatniego skanowania, liczba wykrytych zagrożeń, liczba obiektów, których wyleczenie się nie powiodło, dostępność i stan komponentów aplikacji, godzina ostatniej aktualizacji i wersja antywirusowych baz danych, szczegóły dotyczące zadań i ustawień aplikacji Kaspersky, informacje o aktywnym i zapasowym kluczu licencyjnym, data i identyfikator instalacji aplikacji.

  - Statystyki działania aplikacji: zdarzenia dotyczące zmian w stanie komponentów aplikacji Kaspersky na zarządzanym urządzeniu i wykonywanie zadań zainicjowanych przez komponenty aplikacji.

  - Stan urządzenia zdefiniowany przez aplikację Kaspersky.

  - Znaczniki przypisane przez aplikację Kaspersky.

  - Zestaw zainstalowanych i stosowanych aktualizacji dla aplikacji firmy Kaspersky.

- Dane znajdujące się w zdarzeniach z komponentów Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky. Agent sieciowy przesyła dane z urządzenia na Serwer administracyjny.

- Dane niezbędne do integracji Kaspersky Security Center z systemem SIEM w celu eksportowania zdarzeń. Użytkownik wprowadza dane w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.

- Ustawienia komponentów Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky, przedstawionych w zasadach i profilach zasad. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Ustawienia zadania komponentów Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Dane przetwarzane przez funkcję Zarządzanie lukami i poprawkami. Agent sieciowy przesyła dane wymienione poniżej z urządzenia na Serwer administracyjny:

- Szczegóły dotyczące aplikacji i poprawek zainstalowanych na zarządzanych urządzeniach (Rejestr aplikacji).
- Informacje o sprzęcie wykrytym na zarządzanych urządzeniach (Rejestr sprzętu).
- Szczegóły dotyczące luk w oprogramowaniu innej firmy wykrytych na zarządzanych urządzeniach.
- Szczegóły dotyczące aktualizacji dostępnych dla aplikacji innych firm, zainstalowanych na zarządzanych urządzeniach.
- Szczegóły dotyczące aktualizacji firmy Microsoft, wykrytych przez funkcję WSUS.
- Lista aktualizacji firmy Microsoft, wykrytych przez funkcję WSUS, która musi zostać zainstalowana na urządzeniu.

- Dane wymagane do pobrania aktualizacji na izolowanym serwerze administracyjnym w celu naprawienia luk w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach. Użytkownik wprowadza i przesyła dane za pomocą narzędzia klscflag serwera administracyjnego.
- Dane niezbędne do pracy Kaspersky Security Center ze środowiskami chmury (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). Użytkownik wprowadza dane w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console.
- Kategorie użytkownika dla aplikacji. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.
- Szczegóły plików wykonywalnych wykrytych na zarządzanych urządzeniach przez funkcję Kontroli aplikacji. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.
- Szczegóły dotyczące plików w Kopii zapasowej. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.
- Szczegóły dotyczące plików w Kwarantannie. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.
- Szczegóły dotyczące plików, o które poprosili specjaliści z Kaspersky, w celu przeprowadzenia szczegółowej analizy. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.
- Szczegóły dotyczące stanu i wyzwolenia reguł Adaptacyjnej kontroli anomalii. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.
- Szczegóły dotyczące urządzeń zewnętrznych (jednostki pamięci, informacje o narzędziach do przenoszenia danych, informacje o narzędziach do drukowania oraz magistrale połączeń), zainstalowane lub podłączone do zarządzanego urządzenia i wykryte przez funkcję Kontroli urządzeń. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.
- Informacje o zaszyfrowanych urządzeniach i stanie szyfrowania. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego.
- Szczegóły dotyczące błędów szyfrowania danych na urządzeniach, wykonane przy użyciu funkcji Szyfrowanie danych z aplikacji firmy Kaspersky. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Lista zarządzanych programowalnych sterowników logicznych (PLC). Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Dane wymagane do utworzenia łańcucha rozprzestrzeniania się zagrożeń. Zarządzana aplikacja przesyła dane z urządzenia na Serwer administracyjny poprzez Agenta sieciowego. Pełna lista danych jest dostarczona w plikach pomocy odpowiedniej aplikacji.

- Dane wymagane do integracji Kaspersky Security Center z usługą Kaspersky Managed Detection and Response (dedykowana wtyczka musi być zainstalowana dla Kaspersky Security Center Web Console): token inicjujący integrację, token integracji i token sesji użytkownika. Użytkownik wprowadza token inicjujący integrację w interfejsie konsoli Kaspersky Security Center Web Console. Usługa Kaspersky MDR przesyła token integracji i token sesji użytkownika za pośrednictwem dedykowanej wtyczki.

- Szczegóły wprowadzonych kodów aktywacyjnych lub określonych plików kluczy. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Konta użytkowników: nazwa, opis, imię i nazwisko, adres e-mail, główny numer telefonu, hasło, tajny klucz wygenerowany przez Serwer administracyjny oraz hasło jednorazowe do weryfikacji dwuetapowej. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Dane, których Identity and Access Manager potrzebuje do scentralizowanego uwierzytelniania i dostarczania technologii Single Sign-on (SSO) między aplikacjami Kaspersky zintegrowanymi z Kaspersky Security Center: ustawienia instalacji i konfiguracji Identity and Access Manager, sesja użytkownika Identity and Access Manager, tokeny Identity and Access Manager, stany programu klienckiego i stany serwera zasobu. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Historia rewizji zarządzanych obiektów. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Rejestr usuniętych zarządzanych obiektów. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Pakiety instalacyjne utworzone z pliku, a także ustawienia instalacji. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Dane wymagane do wyświetlania ogłoszeń z Kaspersky w Kaspersky Security Center Web Console. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Dane wymagane do działania wtyczek zarządzanych aplikacji w konsoli Kaspersky Security Center Web Console i zapisywane przez wtyczki w bazie danych Serwera administracyjnego podczas ich rutynowego działania. Opis i sposoby podawania danych znajdują się w plikach pomocy odpowiedniej aplikacji.

- Ustawienia użytkownika Kaspersky Security Center Web Console: wersja językowa oraz temat interfejsu, ustawienia wyświetlania panelu Monitorowanie, informacje o stanie powiadomień (Przeczytane / Nieprzeczytane), stan kolumn w arkuszach kalkulacyjnych (Pokaż / Ukryj), postęp trybu Uczenie. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center Web Console.

- Dziennik zdarzeń aplikacji Kaspersky dla komponentów Kaspersky Security Center i zarządzanej aplikacji firmy Kaspersky. Dziennik zdarzeń aplikacji Kaspersky jest przechowywany na każdym urządzeniu i nie jest nigdy przesyłany na Serwer administracyjny.

- Certyfikaty dla bezpiecznego podłączania zarządzanych urządzeń do komponentów Kaspersky Security Center. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center Web Console.

- Dane wymagane do działania Kaspersky Security Center w środowiskach chmury, takich jak Amazon Web Services (AWS), Microsoft Azure, Google Cloud i Yandex.Cloud. Serwer administracyjny otrzymuje dane z

maszyny wirtualnej, na której działa.

- Informacja o akceptacji przez Użytkownika warunków umów prawnych z Kaspersky.
- Dane serwera administracyjnego, które użytkownik wprowadza w następujących składnikach:
  - Konsola administracyjna
  - Kaspersky Security Center Web Console
  - Terminal wiersza polecenia podczas korzystania z narzędzia klscflag
  - Składniki współpracujące z serwerem administracyjnym za pośrednictwem obiektów automatyzacji klakaut i Kaspersky Security Center OpenAPI
- Wszelkie dane, jakie Użytkownik wprowadza w Konsoli administracyjnej lub interfejsie konsoli Kaspersky Security Center Web Console.

Dane wymienione powyżej mogą zostać przedstawione w Kaspersky Security Center, jeśli stosowana jest jedna z następujących metod:

- Użytkownik wprowadza dane w interfejsie następujących składników:
  - Konsola administracyjna
  - Kaspersky Security Center Web Console
  - Terminal wiersza polecenia podczas korzystania z narzędzia klscflag
  - Składniki współpracujące z serwerem administracyjnym za pośrednictwem obiektów automatyzacji klakaut i Kaspersky Security Center OpenAPI
- Agent sieciowy automatycznie pobiera dane z urządzenia i przesyła je na Serwer administracyjny.
- Agent sieciowy pobiera dane otrzymane przez zarządzaną aplikację firmy Kaspersky i przesyła je na Serwer administracyjny. Listy danych przetwarzanych przez zarządzane aplikacje firmy Kaspersky są dostarczane w plikach pomocy dla odpowiednich aplikacji.
- Serwer administracyjny i Agent sieciowy wskazani jako punkt dystrybucji zbierają informacje o urządzeniach w sieci.
- Dane są przesyłane z urządzenia mobilnego do Serwera administracyjnego przy użyciu protokołu Exchange ActiveSync lub iOS MDM.

Wymienione dane są przechowywane w bazie danych Serwera administracyjnego. Nazwy użytkowników i hasła są przechowywane w postaci zaszyfrowanej.

Wszystkie wymienione dane mogą być przesyłane do Kaspersky tylko poprzez pliki zrzutów, pliki śledzenia lub pliki raportów komponentów Kaspersky Security Center, w tym pliki raportów utworzone przez instalatory i narzędzia.

Pliki zrzutów, pliki śledzenia i pliki raportów komponentów Kaspersky Security Center zawierają losowe dane Serwera administracyjnego, Agenta sieciowego, Konsoli administracyjnej, serwera iOS MDM, serwera urządzeń mobilnych Exchange oraz Kaspersky Security Center Web Console. Te pliki mogą zawierać szczegóły osobiste oraz dane wrażliwe. Pliki zrzutów, pliki śledzenia oraz pliki raportów na urządzeniu w postaci niezaszyfrowanej. Pliki zrzutów, pliki śledzenia i pliki raportów nie są przesyłane do Kaspersky automatycznie; jednakże administrator może przesyłać dane do Kaspersky ręcznie na prośbę pomocy technicznej, aby rozwiązać problemy związane z działaniem Kaspersky Security Center.

Klikając odnośniki w Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console, Użytkownik wyraża zgodę na automatyczne przesyłanie następujących danych:

- Kod Kaspersky Security Center
- Wersja Kaspersky Security Center
- Lokalizacja Kaspersky Security Center
- Identyfikator licencji
- Typ licencji
- Czy licencja została zakupiona u partnera

Lista danych dostarczonych za pośrednictwem odnośników zależy od celu i lokalizacji odnośnika.

Firma Kaspersky wykorzystuje uzyskane dane tylko jako ogólne statystyki. Ogólne statystyki są generowane automatycznie z otrzymanych informacji i nie zawierają żadnych danych osobowych ani poufnych informacji. Jak tylko nowe dane zostaną zebrane, poprzednie dane zostaną usunięte (raz na rok). Statystyki podsumowujące są przechowywane cały czas.

Firma Kaspersky chroni wszelkie zebrane informacje zgodnie z prawem oraz obowiązującymi przepisami stosowanymi w firmie Kaspersky. Dane są przesyłane za pośrednictwem bezpiecznego kanału.

Opcje licencjonowania Kaspersky Security Center

W Kaspersky Security Center licencja może odnosić się do różnych grup funkcji.

Podczas dodawania klucza licencyjnego w oknie właściwości Serwera administracyjnego upewnij się, że dodasz klucz licencyjny, który umożliwia użycie Kaspersky Security Center. Możesz odszukać te informacje na stronie internetowej firmy Kaspersky. Każda strona internetowa rozwiązania zawiera listę aplikacji znajdujących się w rozwiązaniu. Serwer administracyjny może zaakceptować nieobsługiwane klucze licencyjne, na przykład klucz licencyjny dla Kaspersky Endpoint Security Cloud, ale funkcjonalność Kaspersky Security Center w takich przypadkach nie jest obsługiwana.

Podstawowe funkcje Konsoli administracyjnej

Dostępne są następujące funkcje:

- Tworzenie wirtualnych Serwerów administracyjnych, które są używane do zarządzania siecią zdalnych biur lub organizacji klientów.
- Tworzenie hierarchii grup administracyjnych w celu zarządzania określonymi urządzeniami jako pojedynczą jednostką.
- Kontrola stanu ochrony antywirusowej firmy.
- Zdalna instalacja aplikacji.
- Wyświetlanie listy obrazów systemów operacyjnych dostępnych do zdalnej instalacji.
- Scentralizowana konfiguracja aplikacji zainstalowanych na urządzeniach klienckich.

- Przeglądanie i modyfikowanie istniejących grup licencjonowanych aplikacji.
- Statystyki i raporty z działania aplikacji, a także powiadomienia o zdarzeniach krytycznych.
- Zarządzanie szyfrowaniem i ochroną danych.
- Wyświetlanie i ręczne modyfikowanie listy komponentów sprzętu wykrytych poprzez przeszukiwanie sieci.
- Scentralizowana praca z plikami przeniesionymi do Kwarantanny lub Kopii zapasowej i plikami, których przetwarzanie zostało odroczone.
- Zarządzanie rolami użytkownika.

Kaspersky Security Center z obsługą podstawowej funkcjonalności Konsoli administracyjnej jest dostarczany jako część aplikacji Kaspersky do ochrony sieci firmowych. Można ją również pobrać ze strony firmy Kaspersky.

Przed aktywacją aplikacji lub po wygaśnięciu licencji komercyjnej, Kaspersky Security Center zapewnia tylko podstawowe funkcje Konsoli administracyjnej.

Funkcja Zarządzanie lukami i poprawkami

Dostępne są następujące funkcje:

- Zdalna instalacja systemów operacyjnych.
- Zdalna instalacja aktualizacji oprogramowania, skanowanie i naprawianie luk.
- Inwentaryzacja sprzętu.
- Zarządzanie grupą licencjonowanych aplikacji.
- Możliwość zdalnego połączenia z urządzeniami klienckimi poprzez komponent systemu Microsoft® Windows® o nazwie Podłączanie pulpitu zdalnego.
- Nawiązywanie zdalnego połączenia z urządzeniami klienckimi poprzez udostępnianie pulpitu Windows.

Jednostką zarządzająca dla Zarządzanie lukami i poprawkami jest urządzenie klienckie w grupie Zarządzane urządzenia.

Szczegółowe informacje o sprzęcie urządzeń są dostępne podczas procesu inwentaryzacji jako część funkcji Zarządzanie lukami i poprawkami. Aby Zarządzanie lukami i poprawkami działało prawidłowo, na dysku powinno być przynajmniej 100 GB wolnego miejsca.

Funkcja Zarządzanie urządzeniami mobilnymi

Funkcja Zarządzanie urządzeniami mobilnymi jest wykorzystywana do zarządzania urządzeniami mobilnymi Exchange ActiveSync (EAS) i iOS MDM.

Dla urządzeń mobilnych Exchange ActiveSync dostępne są następujące funkcje:

- Tworzenie i modyfikowanie profili zarządzania urządzeniami mobilnymi, przypisywania profili do skrzynek pocztowych użytkowników.

- Konfiguracja ustawień urządzeń mobilnych (synchronizacja poczty, korzystanie z aplikacji, hasło użytkownika, szyfrowanie danych i podłączanie dysków wymiennych).
- Instalacja certyfikatów na urządzeniach mobilnych.

Dla urządzeń iOS MDM dostępne są następujące funkcje:

- Tworzenie i modyfikowanie profili konfiguracyjnych oraz instalowanie profili konfiguracyjnych na urządzeniach mobilnych.
- Instalowanie aplikacji na urządzeniach mobilnych za pośrednictwem App Store® lub plików manifestu (.plist).
- Blokowanie urządzeń mobilnych, resetowanie hasła urządzenia mobilnego oraz usuwanie z niego wszystkich danych.

Dodatkowo, funkcja Zarządzanie urządzeniami mobilnymi umożliwia wykonywanie poleceń udostępnionych przez odpowiednie protokoły.

Jednostką zarządzającą funkcji Zarządzanie urządzeniami mobilnymi jest urządzenie mobilne. Urządzenie mobilne jest zarządzane po jego podłączeniu do serwera urządzeń mobilnych.

Kontrola dostępu oparta o rolę

Kaspersky Security Center oferuje możliwości dla dostępu opartego na roli do funkcji Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky.

Możesz skonfigurować uprawnienia dostępu do funkcji aplikacji dla użytkowników Kaspersky Security Center w jeden z następujących sposobów:

- Konfigurując uprawnienia dla każdego użytkownika lub grupy użytkowników indywidualnie.
- Tworząc standardowe role użytkownika z predefiniowanym zestawem uprawnień i przypisując te role do użytkowników w zależności od ich zakresu obowiązków.

Instalacja systemów operacyjnych i aplikacji

Kaspersky Security Center umożliwia tworzenie obrazów systemów operacyjnych i instalowanie ich na urządzeniach klienckich w sieci, a także wykonywanie zdalnej instalacji aplikacji firmy Kaspersky lub innych producentów. Możesz przechwytywać obrazy systemów operacyjnych z urządzeń i przesyłać je do Serwera administracyjnego. Takie obrazy systemów operacyjnych są przechowywane na Serwerze administracyjnym w dedykowanym folderze. Obraz systemu operacyjnego odpowiedniego urządzenia może zostać przechwycony i utworzony przy użyciu zadania tworzenia pakietu instalacyjnego. Możesz użyć przechwyconych obrazów do zainstalowania ich na nowych urządzeniach w sieci, na których nie zainstalowano jeszcze systemu operacyjnego. W tym przypadku wykorzystywana jest technologia Preboot eXecution Environment (PXE).

Integracja ze środowiskami chmury

Kaspersky Security Center współpracuje nie tylko z urządzeniami lokalnymi, ale zapewnia również specjalne funkcje do pracy w środowisku chmury, takie jak konfiguracja środowiska chmury. Kaspersky Security Center działa z następującymi maszynami wirtualnymi:

- Instancje Amazon EC2

- Maszyny wirtualne Microsoft Azure
- Instancje maszyn wirtualnych Google Cloud

Eksportowanie zdarzeń do systemów SIEM: QRadar firmy IBM i Micro Focus firmy ArcSight

Eksportowanie zdarzeń może być używane w obrębie scentralizowanych systemów, które zajmują się problemami z bezpieczeństwem na poziomie organizacyjnym i technicznym, zapewniają usługi monitorowania ochrony oraz skonsolidowane informacje z różnych rozwiązań. To są systemy SIEM, które oferują przeprowadzania w czasie rzeczywistym analizy ostrzeżeń i zdarzeń zabezpieczeń, wygenerowanych przez aplikacje i sprzęt w sieci, lub Security Operation Centers (SOCs).

Dzięki specjalnej licencji możesz użyć protokołów CEF i LEEF, aby wyeksportować ogólne zdarzenia do systemów SIEM, a także zdarzenia przesyłane przez aplikacje Kaspersky do Serwera administracyjnego.

LEEF (Log Event Extended Format) to dostosowany format zdarzeń dla IBM Security QRadar SIEM. QRadar może integrować, identyfikować i przetwarzać zdarzenia LEEF. Zdarzenia LEEF muszą używać kodowania UTF-8. Szczegółowe informacje na temat protokołu LEEF można znaleźć w Centrum wiedzy IBM.

CEF (Common Event Format) to standard zarządzania dziennikami, który ulepsza współdziałanie informacji dotyczących bezpieczeństwa między różnymi urządzeniami i aplikacjami sieciowymi i zabezpieczającymi. CEF umożliwia korzystanie z podstawowego formatu dziennika zdarzeń, co ułatwia integrowanie i gromadzenie danych do analizy przez system zarządzania korporacji. Systemy ArcSight i Splunk SIEM używają tego protokołu.

Informacje o ograniczeniach głównych funkcji

Przed aktywacją aplikacji lub po wygaśnięciu licencji komercyjnej, Kaspersky Security Center zapewnia podstawowe funkcje Konsoli administracyjnej. Ograniczenia podstawowego działania aplikacji zostały opisane poniżej.

Zarządzanie urządzeniami mobilnymi

Nie można utworzyć nowego profilu i przypisać go do urządzenia mobilnego (iOS MDM) lub skrzynki pocztowej (Exchange ActiveSync). Funkcje zmian istniejących profili oraz przypisywania profili do skrzynek pocztowych są zawsze dostępne.

Zarządzanie aplikacjami

Nie można uruchomić zadania instalacji aktualizacji i zadania usuwania aktualizacji. Wszystkie zadania, które zostały uruchomione przed wygaśnięciem licencji, zostaną zakończone, ale ostanie uaktualnienia nie zostaną zainstalowane. Na przykład, jeśli zadanie instalacji krytycznych uaktualnień zostało uruchomione przed wygaśnięciem licencji, zainstalowane zostaną tylko krytyczne uaktualnienia, które zostały odnalezione przed wygaśnięciem licencji.

Funkcje uruchamiania i modyfikacji synchronizacji, wykrywania luk oraz zadania aktualizacji bazy luk są zawsze dostępne. Nie ma również żadnych ograniczeń wyświetlania, wyszukiwania i sortowania wpisów na liście luk i uaktualnień.

Zdalna instalacja systemów operacyjnych i aplikacji

Zadania przechwytywania i instalowania obrazu systemu operacyjnego nie mogą zostać uruchomione. Zadania, które zostały uruchomione przed wygaśnięciem licencji, zostają zakończone.

Inwentaryzacja sprzętu

Nie można uzyskać żadnych informacji o nowych urządzeniach za pośrednictwem serwera urządzeń mobilnych. Aktualizowane są informacje o komputerach i podłączonych urządzeniach.

Powiadomienia o zmianach w konfiguracji urządzeń nie są wysyłane.

Lista sprzętu jest dostępna do przeglądania i modyfikowania.

Zarządzanie grupą licencjonowanych aplikacji

Nie można dodać nowego klucza licencyjnego.

Powiadomienia o naruszeniach ograniczeń korzystania z kluczy licencyjnych nie są wysyłane.

Zdalne podłączanie do urządzeń klienckich

Zdalne podłączanie do urządzeń klienckich nie jest dostępne.

Ochrona antywirusowa

Program antywirusowy używa baz danych zainstalowanych przed wygaśnięciem licencji.

Integracja ze środowiskami chmury

Jeśli pracujesz w środowisku chmury, nie możesz korzystać z narzędzi AWS, Azure lub Google API dla przeszukiwania segmentów chmury i instalacji aplikacji na urządzeniach. Elementy interfejsu, które wyświetlają funkcje specyficzne dla pracy w środowisku chmury również nie są dostępne.

Funkcje licencjonowania Kaspersky Security Center i zarządzanych aplikacji

Licencjonowanie Serwera administracyjnego i zarządzanych aplikacji posiada następujące specjalne funkcje:

- Możesz dodać klucz licencyjny lub ważny kod aktywacyjny do Serwera administracyjnego, aby aktywować Zarządzanie lukami i poprawkami, Zarządzanie urządzeniami mobilnymi lub Integracja z systemami SIEM. Niektóre funkcje Kaspersky Security Center są dostępne tylko w zależności od aktywnych plików kluczy lub ważnych kodów aktywacyjnych dodanych do Serwera administracyjnego.
- Do repozytorium Serwera administracyjnego można dodać kilka kodów aktywacyjnych i plików kluczy dla zarządzanych aplikacji.

Informacje o licencjonowaniu Kaspersky Security Center

Jeśli aktywowano jedną z licencjonowanych funkcji (na przykład, Zarządzanie urządzeniami mobilnymi) przy użyciu pliku klucza, ale chcesz też korzystać z innej licencjonowanej funkcji (na przykład, Zarządzania lukami i poprawkami), musisz kupić u swojego dostawcy usługi plik klucza, który aktywuje obie te funkcje, i musisz aktywować Serwer administracyjny przy użyciu tego pliku klucza.

Funkcje licencjonowania zarządzanych aplikacji

Licencjonowanie zarządzanych aplikacji obejmuje wdrożenie kodu aktywacyjnego lub pliku klucza automatycznie lub w inny dogodny sposób. W celu wdrożenia kodu aktywacyjnego lub pliku klucza można zastosować następujące metody:

- Automatyczne rozsyłanie

  > Jeśli używasz różnych zarządzanych aplikacji i musisz rozesłać określony plik klucza lub kod aktywacyjny na urządzenia, zdecyduj się na inne sposoby wdrożenia tego kodu aktywacyjnego lub pliku klucza.

  Kaspersky Security Center umożliwia automatyczne rozesłanie dostępnych kluczy licencyjnych na urządzenia. Na przykład, trzy klucze licencyjne są przechowywane w repozytorium Serwera administracyjnego. Zaznaczyłeś pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** dla wszystkich trzech kluczy licencyjnych. Aplikacja zabezpieczająca Kaspersky—na przykład Kaspersky Endpoint Security for Windows—jest zainstalowana na urządzeniach w organizacji. Zostanie wykryte nowe urządzenie, do którego musi być rozesłany klucz licencyjny. Aplikacja określi, na przykład, że na urządzeniu mogą zostać zastosowane dwa klucze licencyjne z repozytorium: klucz licencyjny o nazwie *Key_1* oraz klucz licencyjny o nazwie *Key_2*. Jeden z tych kluczy licencyjnych zostanie zastosowany na urządzeniu. W tym przypadku nie można przewidzieć, który z dwóch kluczy licencyjnych zostanie rozesłany na urządzenie, ponieważ automatyczne rozesłanie kluczy licencyjnych nie oferuje administratorowi podejmowania żadnych działań.

  Podczas rozsyłania klucza licencyjnego urządzenia są zliczane dla tego klucza licencyjnego. Musisz upewnić się, że liczba urządzeń, na których klucz licencyjny został zastosowany, nie przekracza limitu określonego przez licencję. Jeśli liczba urządzeń przekracza limit określony przez licencję, wszystkie urządzenia, które nie zostały objęte licencją, otrzymają stan *Krytyczny*.

- Dodawanie pliku klucza lub kodu aktywacyjnego do pakietu instalacyjnego zarządzanej aplikacji

  Jeśli instalujesz zarządzaną aplikację przy użyciu pakietu instalacyjnego, możesz określić kod aktywacyjny lub plik klucza w tym pakiecie instalacyjnym lub w zasadzie aplikacji. Klucz licencyjny zostanie rozesłany na zarządzane urządzenia podczas kolejnej synchronizacji urządzenia z Serwerem administracyjnym.

- Rozesłanie poprzez zadanie dodaj klucz licencyjny dla zarządzanej aplikacji

  Jeśli zdecydujesz się na użycie zadania dodaj klucz licencyjny dla zarządzanej aplikacji, możesz wybrać klucz licencyjny, który musi zostać rozesłany na urządzenia, oraz wybrać urządzenia w dowolny sposób—na przykład, wybierając grupę administracyjną lub wybór urządzeń.

- Ręczne dodawanie kodu aktywacyjnego lub pliku klucza do urządzeń

Aplikacje Kaspersky. Zdalna instalacja

Ta sekcja opisuje metody zdalnej instalacji aplikacji firmy Kaspersky i ich usuwanie z urządzeń w sieci.

> Przed zainstalowaniem aplikacji na urządzeniach klienckich należy upewnić się, że sprzęt i oprogramowanie tych urządzeń klienckich spełniają stosowne wymagania.

Agent sieciowy jest składnikiem umożliwiającym łączenie się Serwera administracyjnego z urządzeniami klienckimi. Dlatego też Agent sieciowy musi być zainstalowany na każdym urządzeniu klienckim, które będzie połączone ze zdalnym scentralizowanym systemem kontroli. Urządzenie, na którym jest zainstalowany Serwer administracyjny, może użyć tylko wersji serwerowej Agenta sieciowego. Ta wersja jest częścią Serwera administracyjnego, która jest z nim instalowana i usuwana. Nie ma konieczności instalowania Agenta sieciowego na tym urządzeniu.

Agent sieciowy może być instalowany lokalnie lub zdalnie podobnie jak każda inna aplikacja. Podczas scentralizowanego wdrażania aplikacji zabezpieczających poprzez Konsolę administracyjną możesz zainstalować Agenta sieciowego wraz z tymi aplikacjami zabezpieczającymi.

Agenty sieciowe mogą się różnić w zależności od aplikacji Kaspersky, z którymi pracują. W niektórych przypadkach Agent sieciowy może być instalowany tylko lokalnie (w celu uzyskania szczegółowych informacji przeczytaj dokumentację dla konkretnej aplikacji). Wystarczy tylko raz zainstalować Agenta sieciowego na urządzeniu klienckim.

Aplikacje firmy Kaspersky są zarządzane poprzez Konsolę administracyjną przy użyciu wtyczek administracyjnych. Dlatego, aby mieć dostęp do interfejsu do zarządzania aplikacjami poprzez Kaspersky Security Center, na stacji roboczej administratora należy zainstalować odpowiednią wtyczkę administracyjną.

Możesz przeprowadzić zdalną instalację aplikacji ze stacji roboczej administratora w oknie głównym Kaspersky Security Center.

Aby zdalnie zainstalować oprogramowanie, musisz utworzyć zadanie zdalnej instalacji.

Utworzone zadanie zdalnej instalacji zostanie uruchomione zgodnie z jego terminarzem. Możesz przerwać instalację, ręcznie zatrzymując wykonywanie zadania.

Jeśli zdalna instalacja aplikacji zwróciła błąd, możesz sprawdzić, co spowodowało ten błąd i naprawić go przy pomocy narzędzia do przygotowywania zdalnej instalacji.

Możesz monitorować proces zdalnej instalacji aplikacji firmy Kaspersky w sieci, korzystając z raportu ze zdalnej instalacji.

W celu uzyskania bardziej szczegółowych informacji o zarządzaniu wymienionymi aplikacjami za pośrednictwem Kaspersky Security Center zajrzyj do dokumentacji dla konkretnej aplikacji.

Zastępowanie aplikacji zabezpieczających firm trzecich

Instalacja aplikacji zabezpieczających firmy Kaspersky poprzez Kaspersky Security Center może wymagać usunięcia oprogramowania firmy trzeciej niekompatybilnego z instalowaną aplikacją. Kaspersky Security Center oferuje kilka sposobów usunięcia aplikacji firm trzecich.

Usuwanie niekompatybilnych aplikacji przy użyciu instalatora

Ta opcja jest dostępna tylko w Konsoli administracyjnej opartej na konsoli Microsoft Management Console.

Metoda instalatora dotycząca usuwania niekompatybilnych aplikacji jest obsługiwana przez różne typy instalacji. Przed zainstalowaniem aplikacji zabezpieczającej wszystkie niekompatybilne aplikacje są usuwane automatycznie, jeśli w oknie właściwości pakietu instalacyjnego tej aplikacji zabezpieczającej (sekcja **Niekompatybilne aplikacje**) wybrano opcję **Automatycznie odinstaluj niekompatybilne aplikacje**.

Usuwanie niekompatybilnych aplikacji podczas konfigurowania zdalnej instalacji aplikacji

Możesz włączyć opcję **Automatycznie odinstaluj niekompatybilne aplikacje**, gdy konfigurujesz zdalną instalację aplikacji zabezpieczającej. W Konsoli administracyjnej opartej na Microsoft Management Console (MMC) ta opcja jest dostępna w kreatorze zdalnej instalacji. W Kaspersky Security Center Web Console tę opcję można znaleźć w kreatorze wdrażania ochrony. Jeśli ta opcja jest włączona, Kaspersky Security Center usunie niekompatybilne aplikacje przed zainstalowaniem aplikacji zabezpieczającej na zarządzanym urządzeniu.

Dostępne instrukcje:

- Konsola administracyjna: Instalowanie aplikacji przy pomocy kreatora zdalnej instalacji
- Kaspersky Security Center Web Console: Usuwanie niekompatybilnych aplikacji przed instalacją

Dezinstalowanie niekompatybilnych aplikacji przy użyciu dedykowanego zadania

Aby usunąć niekompatybilne aplikacje, użyj zadania **Zdalna dezinstalacja aplikacji**. Zadanie to powinno być uruchomione przed zadaniem instalacji aplikacji zabezpieczającej. Na przykład, w zadaniu instalacji możesz wybrać opcję terminarza **Po zakończeniu wykonywania innego zadania**, gdzie inne zadanie to **Zdalna dezinstalacja aplikacji**.

Ta metoda dezinstalacji jest przydatna, jeśli instalator aplikacji zabezpieczającej nie może skutecznie usunąć niekompatybilnej aplikacji.

Instrukcje dotyczące Konsoli administracyjnej: Tworzenie zadania.

Instalowanie aplikacji przy pomocy zadania zdalnej instalacji

Kaspersky Security Center umożliwia zdalne instalowanie aplikacji na urządzeniach przy użyciu zadań zdalnej instalacji. Te zadania są tworzone i przydzielane do urządzeń za pośrednictwem dedykowanego kreatora. W celu szybkiego i łatwego przypisywania zadań do urządzeń, należy wskazać urządzenia w oknie kreatora w jeden z następujących sposobów:

- **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**. W tym przypadku zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**. Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.
- **Przypisz zadanie do wyboru urządzeń**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonym wyborze. Możesz określić domyślny wybór lub niestandardowy wybór, który utworzyłeś.
- **Przypisz zadanie do grupy administracyjnej**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonej grupie administracyjnej.

Aby zdalna instalacja została poprawnie przeprowadzona na urządzeniu, na którym nie został zainstalowany Agent sieciowy, muszą być otwarte następujące porty: a) TCP 139 i 445; b) UDP 137 i 138. Domyślnie porty te są otwarte dla wszystkich urządzeń z domeny. Porty te są otwierane automatycznie przy użyciu narzędzia do przygotowania zdalnej instalacji.

Instalowanie aplikacji na wybranych urządzeniach

W celu zainstalowania aplikacji na wybranych urządzeniach:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie urządzenia.
2. Z drzewa konsoli wybierz folder **Zadania**.
3. Uruchom tworzenie zadania, klikając przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center** wybierz **Zdalna instalacja aplikacji** jako typ zadania.

   Kreator tworzenia nowego zadania tworzy Zadanie zdalnej instalacji wybranej aplikacji dla określonych urządzeń. Nowo utworzone zadanie będzie wyświetlane w obszarze roboczym folderu **Zadania**.
4. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji, wybrana aplikacja zostanie zainstalowana na wybranych urządzeniach.

Instalowanie aplikacji na urządzeniach klienckich z grupy administracyjnej

W celu zainstalowania aplikacji na urządzeniach klienckich z grupy administracyjnej:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednią grupę administracyjną.
2. Z drzewa konsoli wybierz grupę administracyjną.
3. W obszarze roboczym grupy wybierz zakładkę **Zadania**.
4. Uruchom tworzenie zadania, klikając przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center** wybierz **Zdalna instalacja aplikacji** jako typ zadania.

   Kreator tworzenia nowego zadania tworzy grupowe Zadanie zdalnej instalacji wybranej aplikacji. Nowe zadanie pojawi się w obszarze roboczym grupy administracyjnej na zakładce **Zadania**.
5. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji, wybrana aplikacja zostanie zainstalowana na urządzeniach klienckich w grupie administracyjnej.

Instalowanie aplikacji przy użyciu zasad grupy Active Directory

Kaspersky Security Center pozwala na instalowanie aplikacji Kaspersky na zarządzanych urządzeniach przy użyciu zasad grupy Active Directory.

Możesz zainstalować aplikacje, korzystając z zasad grupy Active Directory jedynie przy pomocy pakietów instalacyjnych, które zawierają Agenta sieciowego.

W celu zainstalowania aplikacji przy użyciu profili grupy Active Directory:

1. Uruchom konfigurowanie instalacji aplikacji przy użyciu kreatora zdalnej instalacji.
2. W oknie **Określanie ustawień** zadania zdalnej instalacji kreatora zdalnej instalacji wybierz opcję **Przypisz pakiet instalacyjny do zasad grupy Active Directory**.
3. W oknie **Wybierz konta w celu uzyskania dostępu do urządzeń kreatora** zdalnej instalacji wybierz opcję **Konto wymagane (Agent sieciowy nie jest używany)**.
4. Dodaj konto z uprawnieniami administratora na urządzeniu, na którym jest zainstalowany program Kaspersky Security Center, lub konto, które należy do grupy domeny Twórcy-właściciele zasad grupy.
5. Nadaj wybranemu kontu następujące uprawnienia:
   a. Przejdź do **Panel sterowania** → **Narzędzia administracyjne** i otwórz **Zarządzanie zasadami grupy**.
   b. Kliknij węzeł z żądaną domeną.
   c. Kliknij sekcję **Delegowanie**.
   d. Na liście rozwijanej **Uprawnienia** wybierz opcję **Połącz obiekty zasad grupy**.
   e. Kliknij **Dodaj**.
   f. W otwartym oknie **Wybierz Użytkownika, Komputer lub Grupę** wybierz żądane konto.
   g. Kliknij **OK**, aby zamknąć okno **Wybierz Użytkownika, Komputer lub Grupę**.
   h. Na liście **Grupy i użytkownicy** wybierz konto, które zostało dodane, a następnie kliknij **Zaawansowane** → **Zaawansowane**.
   i. Na liście **Wpisy uprawnień** kliknij dwukrotnie konto, które tyle co dodałeś.
   j. Nadaj następujące uprawnienia:
      - **Utwórz obiekty grupy**
      - **Usuń obiekty grupy**
      - **Utwórz obiekty kontenera zasad grupy**
      - **Usuń obiekty kontenera zasad grupy**

k. Kliknij **OK**, aby zachować zmiany.

6. Określ inne ustawienia, postępując zgodnie z instrukcjami kreatora.

7. Uruchom utworzone zadanie zdalnej instalacji ręcznie lub zaczekaj na jego uruchomienie zgodne z terminarzem.

Rozpocznie się następująca sekwencja zdalnej instalacji:

1. Po uruchomieniu zadania, w każdej domenie, do której należą urządzenia klienckie z określonego zbioru, zostaną utworzone następujące obiekty:

   - Obiekt zasad grupy (GPO) o nazwie **Kaspersky_AK{GUID}**.

   - Grupa bezpieczeństwa, która odpowiada GPO. Ta grupa bezpieczeństwa zawiera urządzenia klienckie objęte zadaniem. Zawartość grupy bezpieczeństwa określa zakres GPO.

2. Kaspersky Security Center instaluje wybrane aplikacje firmy Kaspersky na urządzeniach klienckich bezpośrednio z sieciowego folderu współdzielonego Share. W folderze instalacyjnym Kaspersky Security Center zostanie utworzony pomocniczy podfolder, zawierający plik .msi potrzebny do zainstalowania aplikacji.

3. Po dodaniu nowych urządzeń do obszaru zadania, są one dodawane do grupy bezpieczeństwa podczas kolejnego uruchomienia zadania. Jeśli w terminarzu uruchamiania zadania wybrana jest opcja **Uruchom pominięte zadania**, urządzenia są dodawane do grupy zabezpieczeń od razu.

4. Po usunięciu urządzeń z obszaru zadania, są one usuwane z grupy zabezpieczeń podczas kolejnego uruchomienia zadania.

5. Po usunięciu zadania z Active Directory, usuwany jest GPO, odnośnik do GPO oraz odpowiadająca mu grupa zabezpieczeń.

Jeżeli chcesz zastosować inny schemat instalacji przy użyciu Active Directory, możesz ręcznie skonfigurować żądane ustawienia. Na przykład, może to być wymagane w następujących wypadkach:

- Jeśli administrator ochrony antywirusowej nie ma uprawnień do wprowadzania zmian w Active Directory pewnych domen

- Jeśli oryginalny pakiet instalacyjny musi być przechowywany w oddzielnym zasobie sieciowym

- Jeśli konieczne jest połączenie GPO z określonymi jednostkami Active Directory

Dostępne są następujące opcje korzystania z alternatywnego scenariusza instalacji poprzez Active Directory:

- W przypadku, gdy instalacja musi być przeprowadzona bezpośrednio z folderu współdzielonego Kaspersky Security Center, we właściwościach GPO musisz określić plik msi zlokalizowany w podfolderze exec folderu pakietu instalacyjnego żądanej aplikacji.

- Jeżeli pakiet instalacyjny ma znajdować się w innym zasobie sieciowym, skopiuj do niego całą zawartość foldera exec. Jest to konieczne, gdyż oprócz pliku z rozszerzeniem .msi folder zawiera pliki konfiguracyjne wygenerowane podczas tworzenia pakietu. W celu zainstalowania aplikacji wraz z kluczem licencyjnym, skopiuj do tego folderu także plik klucza.

Instalowanie aplikacji na podrzędnych Serwerach administracyjnych

W celu zainstalowania aplikacji na podrzędnych Serwerach administracyjnych:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie podrzędne Serwery administracyjne.

2. Upewnij się, że pakiet instalacyjny dla instalowanej aplikacji znajduje się na każdym z wybranych podrzędnych Serwerów administracyjnych. Jeśli na żadnym podrzędnym Serwerze administracyjnym nie można znaleźć pakietu instalacyjnego, roześlij go przy użyciu zadania rozsyłania pakietu instalacyjnego.

3. Utwórz zadanie instalacji aplikacji na podrzędnych Serwerach administracyjnych w jeden z następujących sposobów:

   - Jeśli chcesz utworzyć zadanie dla podrzędnych Serwerów administracyjnych w wybranej grupie administracyjnej, utwórz grupowe zadanie zdalnej instalacji dla tej grupy.

   - Jeśli chcesz utworzyć zadanie dla określonych podrzędnych Serwerów administracyjnych, utwórz zadanie zdalnej instalacji dla określonych urządzeń.

   Zostanie uruchomiony Kreator tworzenia zadania wdrażania, który poprowadzi Cię przez tworzenie zadania zdalnej instalacji. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w sekcji **Serwer administracyjny Kaspersky Security Center** otwórz folder **Zaawansowane** i wybierz **Zdalna instalacja aplikacji na podrzędnych Serwerach administracyjnych** jako typ zadania.

   Kreator tworzenia nowego zadania utworzy Zadanie zdalnej instalacji wybranej aplikacji na określonych podrzędnych Serwerach administracyjnych.

4. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji, wybrana aplikacja zostanie zainstalowana na podrzędnych Serwerach administracyjnych.

Instalowanie aplikacji przy pomocy kreatora zdalnej instalacji

Do zainstalowania aplikacji firmy Kaspersky można użyć kreatora zdalnej instalacji. Kreator zdalnej instalacji umożliwia przeprowadzenie zdalnej instalacji aplikacji przy pomocy specjalnie utworzonych pakietów instalacyjnych lub bezpośrednio z pakietu dystrybucyjnego.

Aby zadanie Zdalnej instalacji zostało poprawnie wykonane na urządzeniu klienckim, na którym nie został zainstalowany Agent sieciowy, muszą być otwarte następujące porty: TCP 139 i 445; UDP 137 i 138. Domyślnie porty te są otwarte dla wszystkich urządzeń z domeny. Porty te są otwierane automatycznie przy użyciu narzędzia do przygotowania zdalnej instalacji.

W celu zainstalowania aplikacji na wybranych urządzeniach przy użyciu kreatora zdalnej instalacji:

1. W drzewie konsoli zlokalizuj folder **Zdalna instalacja**, z którego wybierz podfolder **Pakiety instalacyjne**.

2. W obszarze roboczym folderu wybierz pakiet instalacyjny aplikacji, którą chcesz zainstalować.

3. Z menu kontekstowego pakietu instalacyjnego wybierz **Zainstaluj aplikację**.

   Zostanie uruchomiony Kreator zdalnej instalacji.

4. W oknie **Wybierz urządzenia do instalacji** możesz utworzyć listę urządzeń, na których zostanie zainstalowana aplikacja:

- Zainstaluj w grupie zarządzanych urządzeń

  Jeżeli ta opcja jest zaznaczona, zadanie zdalnej instalacji jest tworzone dla grupy urządzeń.

- Wybierz urządzenia do instalacji

  Jeżeli ta opcja jest zaznaczona, zadanie zdalnej instalacji jest tworzone dla określonych urządzeń. Do tych określonych urządzeń mogą należeć zarządzane urządzenia oraz urządzenia nieprzypisane.

5. W oknie **Określanie ustawień zadania zdalnej instalacji** określ ustawienia zdalnej instalacji aplikacji.

   W grupie ustawień **Wymuś pobranie pakietu instalacyjnego** określ sposób rozsyłania na urządzenia klienckie plików, które są niezbędne do zainstalowania aplikacji:

   - Przy użyciu Agenta sieciowego

     Jeśli ta opcja jest włączona, pakiety instalacyjne są dostarczane na urządzenia klienckie przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

     Jeśli ta opcja jest wyłączona, pakiety instalacyjne są dostarczane przy użyciu narzędzi systemu operacyjnego urządzeń klienckich.

     Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń z zainstalowanymi Agentami sieciowymi.

     Domyślnie opcja ta jest włączona.

   - Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny

     Jeśli ta opcja jest włączona, pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego urządzeń klienckich za pośrednictwem Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci co Serwer administracyjny.

     Domyślnie opcja ta jest włączona.

   - Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji

     Jeśli ta opcja jest włączona, pakiety instalacyjne są przesyłane na urządzenia klienckie przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjnych. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

     Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego są niedostępne.

     Domyślnie ta opcja jest włączona dla zadań zdalnej instalacji utworzonych na wirtualnym Serwerze administracyjnym.

   - Liczba prób instalacji

Jeśli podczas wykonywania zadania Zdalna instalacja programowi Kaspersky Security Center nie uda się zainstalować aplikacji na zarządzanym urządzeniu w obrębie liczby uruchomień instalatora określonych przez parametr, Kaspersky Security Center zatrzyma dostarczanie pakietu instalacyjnego na to zarządzane urządzenie i już nie uruchomi instalatora na urządzeniu.

Opcja `Liczba prób instalacji` umożliwia zachowanie zasobów zarządzanego urządzenia, a także zmniejszenie ruchu sieciowego (dezinstalacja, uruchomienie pliku MSI i wiadomości o błędach).

Powtarzające się próby uruchomienia zadania mogą wskazywać na problem na urządzeniu, który uniemożliwia przeprowadzenie instalacji. Administrator powinien rozwiązać problem w określonej liczbie prób instalacji (na przykład, przydzielając wystarczającą ilość miejsca, usuwając niekompatybilne aplikacje lub modyfikując ustawienia innych aplikacji, które uniemożliwiają przeprowadzenie instalacji) i uruchomić ponownie zadanie (ręcznie lub zgodnie z terminarzem).

Jeśli instalacja się nie powiedzie, problem jest uznawany za nierozwiązalny i wszelkie dalsze uruchomienia zadania są postrzegane jako niepotrzebne zużywanie zasobów i ruchu sieciowego.

Po utworzeniu zadania, licznik prób jest ustawiony na `0`. Każde uruchomienie instalatora, które zwraca błąd na urządzeniu, zwiększa wartość licznika o jeden.

Jeśli liczba prób określonych w parametrze została przekroczona, a urządzenie jest gotowe do zainstalowania aplikacji, możesz zwiększyć wartość parametru `Number of attempts to install` i uruchomić zadanie do zainstalowania aplikacji. W razie czego możesz utworzyć nowe zadanie Zdalna instalacja.

Określ, co należy robić z urządzeniami klienckimi, zarządzanymi przez inny Serwer administracyjny:

- **Zainstaluj na wszystkich urządzeniach**

  Aplikacja zostanie zainstalowana nawet na urządzeniach zarządzanych przez inne Serwery administracyjne.

  Opcja ta jest wybrana domyślnie. Nie musisz zmieniać tego ustawienia, jeśli masz tylko jeden Serwer administracyjny w swojej sieci.

- **Zainstaluj tylko na urządzeniach zarządzanych przez ten Serwer administracyjny**

  Aplikacja zostanie zainstalowana tylko na urządzeniach zarządzanych przez ten Serwer administracyjny. Wybierz tę opcję, jeśli posiadasz więcej niż jeden Serwer administracyjny w swojej sieci i chcesz uniknąć konfliktów między nimi.

Określ ustawienia dodatkowe:

- **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**

  Jeśli ta opcja jest włączona, wybrana aplikacja nie zostanie ponownie zainstalowana, jeśli już jest zainstalowana na tym urządzeniu klienckim.

  Jeśli ta opcja jest wyłączona, aplikacja zostanie zainstalowana mimo wszystko.

  Domyślnie opcja ta jest włączona.

- **Przypisz pakiet instalacyjny do zasad grupy Active Directory**

Jeśli ta opcja jest włączona, pakiet instalacyjny jest instalowany przy użyciu zasad grupy Active Directory.

Ta opcja jest dostępna, jeśli wybrany jest pakiet instalacyjny Agenta sieciowego.

Domyślnie opcja ta jest wyłączona.

6. W oknie **Wybierz klucz licencyjny** wybierz klucz licencyjny i metodę jego dystrybucji:

- **Nie umieszczaj klucza licencyjnego w pakiecie instalacyjnym (zalecane)**

  Klucz jest automatycznie rozsyłany na wszystkie urządzenia, z którymi jest kompatybilny:

  - Jeśli we właściwościach klucza jest włączona automatyczna dystrybucja.
  - Jeśli utworzono zadanie **Dodaj klucz**.

- **Umieść klucz licencyjny w pakiecie instalacyjnym**

  Klucz jest rozsyłany na urządzenia wraz z pakietem instalacyjnym.

  Nie zalecamy rozpowszechniania klucza przy użyciu tej metody, ponieważ współdzielone prawa dostępu do odczytu są włączone do repozytorium pakietów instalacyjnych.

Okno **Wybierz klucz licencyjny** jest wyświetlane, jeśli pakiet instalacyjny nie zawiera klucza licencyjnego.

Jeśli pakiet instalacyjny zawiera klucz licencyjny, zostanie wyświetlone okno **Właściwości klucza licencyjnego** zawierające szczegóły dotyczące klucza licencyjnego.

7. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** określ, czy urządzenia muszą być uruchamiane ponownie, jeśli podczas instalacji aplikacji wymagane jest ponowne uruchomienie systemu operacyjnego:

- **Nie uruchamiaj ponownie urządzenia**

  Jeśli ta opcja jest zaznaczona, urządzenie nie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

- **Uruchom urządzenie ponownie**

  Jeśli ta opcja jest zaznaczona, urządzenie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

- **Pytaj użytkownika o akcję**

  Jeśli ta opcja jest zaznaczona, po zainstalowaniu aplikacji zabezpieczającej wyświetlane jest powiadomienie informujące o konieczności ponownego uruchomienia urządzenia. Po kliknięciu odnośnika **Modyfikuj** możesz zmodyfikować tekst wiadomości, okres wyświetlania wiadomości oraz czas automatycznego ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

- Wymuś zamknięcie aplikacji dla zablokowanych sesji

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie aplikacji na zablokowanych urządzeniach przed ich ponownym uruchomieniem.

  Domyślnie opcja ta jest wyłączona.

8. W oknie **Wybierz konta w celu uzyskania dostępu do urządzeń** możesz dodać konta, które będą używane do uruchamiania zadania Zdalnej instalacji:

   - Konto nie jest wymagane (Agent sieciowy jest zainstalowany)

     Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

     Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

   - Konto wymagane (Agent sieciowy nie jest używany)

     Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisano zadanie zdalnej instalacji. W takim przypadku możesz określić konto użytkownika, aby zainstalować aplikację.

     Aby określić konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji, kliknij przycisk **Dodaj**, wybierz **Konto lokalne**, a następnie określ poświadczenia konta użytkownika.

     Możesz określić kilka kont użytkowników, na przykład, jeśli żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, dla których definiujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

9. W oknie **Uruchamianie instalacji** kliknij przycisk **Dalej**, aby utworzyć i uruchomić zadanie Zdalnej instalacji na wybranych urządzeniach.

   Jeśli w oknie **Uruchamianie instalacji** wybrano opcję **Nie uruchamiaj zadania niezwłocznie po zakończeniu działania kreatora zdalnej instalacji**, zadanie zdalnej instalacji nie zostanie uruchomione. Możesz później uruchomić to zadanie ręcznie. Nazwa zadania odpowiada nazwie pakietu instalacyjnego dla aplikacji: **Instalacja <Nazwa pakietu instalacyjnego>**.

W celu zainstalowania aplikacji na urządzeniach w grupie administracyjnej przy użyciu kreatora zdalnej instalacji:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednią grupę administracyjną.
2. Z drzewa konsoli wybierz grupę administracyjną.
3. W obszarze roboczym grupy kliknij przycisk **Wykonaj akcję** i z listy rozwijalnej wybierz **Zainstaluj aplikację**.

   Zostanie uruchomiony Kreator zdalnej instalacji. Postępuj zgodnie z instrukcjami kreatora.

4. W ostatnim kroku kreatora kliknij **Dalej**, aby utworzyć i uruchomić Zadanie zdalnej instalacji na wybranych urządzeniach.

Po zakończeniu działania kreatora zdalnej instalacji, Kaspersky Security Center wykona następujące czynności:

- Tworzenie pakietu instalacyjnego potrzebnego do zainstalowania aplikacji (jeśli nie został utworzony wcześniej). Pakiet instalacyjny znajduje się w folderze **Zdalna instalacja**, w podfolderze **Pakiety instalacyjne** i nosi nazwę

odpowiadającą nazwie i wersji aplikacji. Możesz użyć tego pakietu instalacyjnego do przyszłej instalacji aplikacji.

- Tworzy i uruchamia zadanie zdalnej instalacji dla określonych urządzeń lub grupy administracyjnej. Utworzone zadanie zdalnej instalacji jest przechowywane w folderze **Zadania** lub jest dodawane do zadań grupy administracyjnej, dla której zostało utworzone. Możesz później uruchomić to zadanie ręcznie. Nazwa zadania odpowiada nazwie pakietu instalacyjnego dla aplikacji: **Instalacja <Nazwa pakietu instalacyjnego>**.

Wyświetlanie raportu wdrażania ochrony

Użyj opcji Raport wdrażania ochrony, aby monitorować postęp zdalnej instalacji ochrony sieci.

W celu wyświetlenia raportu wdrażania ochrony:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. W folderze **Raporty** wybierz szablon raportu o nazwie **Raport wdrażania ochrony**.

Obszar roboczy wyświetla raport zawierający informacje o zdalnej instalacji ochrony na wszystkich urządzeniach w sieci.

Możesz wygenerować nowy raport wdrażania ochrony i określić typy danych, które powinien zawierać:

- Dla grupy administracyjnej
- Dla wskazanych urządzeń
- Dla wyboru urządzeń
- Dla wszystkich urządzeń

Kaspersky Security Center zakłada, że na urządzeniu jest wdrożona ochrona, jeśli jest na nim zainstalowana aplikacja zabezpieczająca oraz jest włączona ochrona w czasie rzeczywistym.

Zdalne usuwanie aplikacji

Kaspersky Security Center umożliwia zdalne odinstalowanie aplikacji z urządzeń przy użyciu zadań zdalnej dezinstalacji. Te zadania są tworzone i przydzielane do urządzeń za pośrednictwem dedykowanego kreatora. W celu szybkiego i łatwego przypisywania zadań do urządzeń, należy wskazać urządzenia w oknie kreatora w jeden z następujących sposobów:

- **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**. W tym przypadku zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**. Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

- **Przypisz zadanie do wyboru urządzeń**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonym wyborze. Możesz określić domyślny wybór lub niestandardowy wybór, który utworzyłeś.

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

Zdalne usuwanie aplikacji z urządzeń klienckich w grupie administracyjnej

W celu zdalnego usunięcia aplikacji z urządzeń klienckich w grupie administracyjnej:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednią grupę administracyjną.

2. Z drzewa konsoli wybierz grupę administracyjną.

3. W obszarze roboczym grupy wybierz zakładkę **Zadania**.

4. Uruchom tworzenie zadania, klikając przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center**, w folderze **Zaawansowane** wybierz **Zdalna dezinstalacja aplikacji** jako typ zadania.

   Kreator tworzenia nowego zadania tworzy grupowe zadanie zdalnej dezinstalacji wybranej aplikacji. Nowe zadanie pojawi się w obszarze roboczym grupy administracyjnej na zakładce **Zadania**.

5. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej dezinstalacji, wybrana aplikacja zostanie odinstalowana z urządzeń klienckich w grupie administracyjnej.

Zdalne usuwanie aplikacji z wybranych urządzeń

W celu zdalnego usunięcia aplikacji z wybranych urządzeń:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie urządzenia.

2. Z drzewa konsoli wybierz folder **Zadania**.

3. Uruchom tworzenie zadania, klikając **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center**, w folderze **Zaawansowane** wybierz **Zdalna dezinstalacja aplikacji** jako typ zadania.

   Kreator tworzenia nowego zadania tworzy zadanie zdalnej dezinstalacji wybranej aplikacji z określonych urządzeń. Nowo utworzone zadanie będzie wyświetlane w obszarze roboczym folderu **Zadania**.

4. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej dezinstalacji, wybrana aplikacja zostanie odinstalowana z wybranych urządzeń.

Praca z pakietami instalacyjnymi

Podczas tworzenia zadań zdalnej instalacji system używa pakietów instalacyjnych zawierających zestawy parametrów potrzebnych do zainstalowania oprogramowania.

Pakiety instalacyjne mogą zawierać plik klucza. Zalecane jest unikanie współdzielenia dostępu do pakietów instalacyjnych zawierających plik klucza.

Możesz użyć jednego pakietu instalacyjnego wiele razy.

Pakiety instalacyjne utworzone dla Serwera administracyjnego zostają przeniesione do drzewa konsoli i znajdują się w folderze **Zdalna instalacja**, w podfolderze **Pakiety instalacyjne**. Pakiety instalacyjne są przechowywane na Serwerze administracyjnym, w podfolderze Pakiety, w obrębie określonego folderu współdzielonego.

Tworzenie pakietu instalacyjnego

W celu utworzenia pakietu instalacyjnego:

1. Nawiąż połączenie z żądanym Serwerem administracyjnym.
2. W drzewie konsoli, w folderze **Zdalna instalacja** wybierz podfolder **Pakiety instalacyjne**.
3. Uruchom tworzenie pakietu instalacyjnego w jeden z następujących sposobów:
   - Wybierając **Nowy** → **Pakiet instalacyjny** z menu kontekstowego folderu **Pakiety instalacyjne**.
   - Wybierając **Utwórz** → **Pakiet instalacyjny** w menu kontekstowym listy pakietów instalacyjnych.
   - Klikając odnośnik **Utwórz pakiet instalacyjny** w sekcji zarządzania listą pakietów instalacyjnych.

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

   Podczas tworzenia pakietu instalacyjnego dla aplikacji firmy Kaspersky może zostać zaproponowane przejrzenie Umowy licencyjnej i Polityki prywatności dla tej aplikacji. Uważnie przeczytaj Umowę licencyjną i Politykę prywatności. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności, wybierz następujące opcje w sekcji **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia następujących**:

   - **Warunki i postanowienia tej Umowy licencyjnej**
   - **Polityka prywatności opisująca zasady przetwarzania danych**

   Instalacja aplikacji na urządzeniu będzie kontynuowana po wybraniu opcji. Tworzenie pakietu instalacyjnego zostanie wznowione. Ścieżka do pliku Umowy licencyjnej i Polityki prywatności jest określona w pliku KUD lub KPD, znajdującym się w pakiecie dystrybucyjnym aplikacji, dla którego tworzony jest pakiet instalacyjny.

Podczas tworzenia pakietu instalacyjnego dla Kaspersky Endpoint Security for Mac możesz wybrać język Umowy licencyjnej i Polityki prywatności.

Podczas tworzenia pakietu instalacyjnego dla aplikacji firmy Kaspersky możesz włączyć automatyczną instalację komponentów systemu (wymagania wstępne) wymaganych do zainstalowania aplikacji. Kreator tworzenia nowego pakietu wyświetla listę wszystkich komponentów systemu dostępnych dla wybranej aplikacji. Jeśli tworzony jest pakiet instalacyjny łaty (niekompletny pakiet dystrybucyjny), lista zawiera wszystkie wymagania wstępne systemu dla instalacji łaty, aż do pełnego pakietu dystrybucyjnego. Lista ta może zostać otwarta w dowolnym momencie we właściwościach pakietu instalacyjnego.

Aktualizacje zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center. Jeśli ta wersja jest nowsza niż aktualna wersja, te aktualizacje są wyświetlane, ale nie można ich zatwierdzić. Ponadto żadne pakiety instalacyjne nie mogą być tworzone z takich aktualizacji, dopóki nie zaktualizujesz Kaspersky Security Center. Zostaniesz poproszony o uaktualnienie instancji Kaspersky Security Center do wymaganej wersji minimalnej.

Po zakończeniu pracy kreatora tworzenia nowego pakietu, nowy pakiet instalacyjny pojawi się w obszarze roboczym folderu **Pakiety instalacyjne**.

Nie ma konieczności ręcznego utworzenia pakietu instalacyjnego dla zdalnej instalacji Agenta sieciowego. Tworzony jest on automatycznie podczas instalacji programu Kaspersky Security Center w folderze **Pakiety instalacyjne**. Jeśli usunięto pakiet do zdalnej instalacji Agenta sieciowego, wówczas do jego odtworzenia niezbędny będzie plik nagent.kud znajdujący się w folderze NetAgent pakietu dystrybucyjnego programu Kaspersky Security Center.

W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.

Podczas tworzenia pakietu instalacyjnego Serwera administracyjnego, jako plik opisu należy wskazać plik sc.kud, znajdujący się w głównym folderze pakietu dystrybucyjnego Kaspersky Security Center.

Tworzenie autonomicznych pakietów instalacyjnych

Ty oraz użytkownicy urządzeń w Twojej organizacji mogą używać autonomicznych pakietów instalacyjnych, aby ręcznie instalować aplikacje na urządzeniach.

Autonomiczny pakiet instalacyjny jest plikiem wykonywalnym (installer.exe), który można umieścić na serwerze sieciowym lub w folderze sieciowym lub przenieść na urządzenie klienckie w dowolny sposób. Możesz także wysłać odnośnik do autonomicznego pakietu instalacyjnego za pośrednictwem poczty elektronicznej. Na urządzeniu klienckim użytkownik może uruchomić otrzymany plik lokalnie, aby zainstalować aplikację bez udziału Kaspersky Security Center.

Upewnij się, że autonomiczny pakiet instalacyjny nie jest dostępny dla nieupoważnionych osób.

Możesz tworzyć autonomiczne pakiety instalacyjne dla aplikacji Kaspersky i aplikacji innych firm na platformy Windows, macOS i Linux. Aby utworzyć autonomiczny pakiet instalacyjny dla aplikacji firmy trzeciej, w pierwszej kolejności powinieneś utworzyć niestandardowy pakiet instalacyjny.

Źródło utworzenia autonomicznych pakietów instalacyjnych to pakiety instalacyjne na liście utworzonej na Serwerze administracyjnym.

W celu utworzenia autonomicznego pakietu instalacyjnego:

1. W drzewie konsoli wybierz **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Na liście pakietów instalacyjnych wybierz pakiet instalacyjny, dla którego chcesz utworzyć pakiet autonomiczny.

3. Z menu kontekstowego wybierz **Utwórz autonomiczny pakiet instalacyjny**.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

4. Na pierwszej stronie kreatora, jeśli wybrano pakiet instalacyjny dla aplikacji Kaspersky i chcesz zainstalować Agenta sieciowego razem z wybraną aplikacją, upewnij się, że opcja **Zainstaluj Agenta sieciowego wraz z aplikacją** jest włączona.

   Domyślnie opcja ta jest włączona. Zalecane jest włączenie tej opcji, jeśli nie jesteś pewien, czy Agent sieciowy jest zainstalowany na urządzeniu. Jeśli Agent sieciowy jest już zainstalowany na urządzeniu, po zainstalowaniu autonomicznego pakietu instalacyjnego wraz z Agentem sieciowym, Agent sieciowy zostanie zaktualizowany do nowszej wersji.

   Jeśli wyłączysz tę opcję, Agent sieciowy nie zostanie zainstalowany na urządzeniu, a urządzenie będzie niezarządzane.

   Jeśli autonomiczny pakiet instalacyjny dla wybranej aplikacji już istnieje na Serwerze administracyjnym, kreator poinformuje o tym fakcie. W tym przypadku powinieneś wybrać jedno z następujących działań:

   - **Utwórz autonomiczny pakiet instalacyjny**. Wybierz tę opcję, na przykład, jeśli chcesz utworzyć autonomiczny pakiet instalacyjny dla nowej wersji aplikacji oraz chcesz zachować autonomiczny pakiet instalacyjny, który utworzyłeś dla poprzedniej wersji aplikacji. Nowy autonomiczny pakiet instalacyjny zostanie umieszczony w innym folderze.

   - **Użyj istniejącego autonomicznego pakietu instalacyjnego**. Wybierz tę opcję, jeśli chcesz użyć istniejącego autonomicznego pakietu instalacyjnego. Proces tworzenia pakietu nie zostanie uruchomiony.

   - **Ponownie skompiluj istniejący autonomiczny pakiet instalacyjny**. Wybierz tę opcję, jeśli ponownie chcesz utworzyć autonomiczny pakiet instalacyjny dla tej samej aplikacji. Autonomiczny pakiet instalacyjny znajduje się w tym samym folderze.

5. W kroku kreatora wybierz opcję **Przenieś nieprzypisane urządzenia do tej grupy** i określ grupę administracyjną, do której chcesz przenieść urządzenie klienckie po zainstalowaniu Agenta sieciowego.

   Domyślnie, urządzenie zostanie przeniesione do grupy **Zarządzane urządzenia**.

   Jeśli nie chcesz przenieść urządzenia klienckiego do grupy administracyjnej po zainstalowaniu Agenta sieciowego, wybierz opcję **Nie przenoś urządzeń**.

6. W kolejnym kroku kreatora, po zakończeniu procesu tworzenia autonomicznego pakietu instalacyjnego, zostanie wyświetlony wynik tworzenia autonomicznego pakietu instalacyjnego oraz ścieżka do pakietu autonomicznego.

   Możesz kliknąć odnośniki i wykonać dowolną z następujących czynności:

   - Otwórz folder z autonomicznym pakietem instalacyjnym.

   - Wyślij e-mail zawierający odnośnik do utworzonego autonomicznego pakietu instalacyjnego. Aby wykonać tę akcję, powinieneś mieć uruchomioną aplikację do obsługi wiadomości e-mail.

- Przykładowy kod HTML do publikacji odnośnika na stronie internetowej. Plik TXT jest tworzony i otwierany w aplikacji, która jest kojarzona z formatem TXT. W pliku wyświetlany jest znacznik HTML <a> z atrybutami.

7. W następnym kroku kreatora, jeśli chcesz otworzyć listę autonomicznych pakietów instalacyjnych, włącz opcję **Otwórz listę pakietów autonomicznych**.

8. Kliknij przycisk **ZAKOŃCZ**.

   Kreator tworzenia autonomicznego pakietu instalacyjnego zostanie zamknięty.

Autonomiczny pakiet instalacyjny jest tworzony i umieszczany w podfolderze Pkglnst folderu współdzielonego Serwera administracyjnego. Możesz przejrzeć listę pakietów autonomicznych, klikając przycisk **Wyświetl listę pakietów autonomicznych** nad listą pakietów instalacyjnych.

Tworzenie niestandardowego pakietu instalacyjnego

W celu wykonania następujących czynności możesz użyć niestandardowych pakietów instalacyjnych:

- Aby zainstalować dowolną aplikację (np. edytor tekstu) na urządzeniu klienckim, na przykład, przy użyciu zadania.
- Aby utworzyć autonomiczny pakiet instalacyjny.

Niestandardowy pakiet instalacyjny to folder z zestawem plików. Źródło utworzenia niestandardowego pakietu instalacyjnego to *plik archiwum*. Plik archiwum zawiera plik lub pliki, które muszą znajdować się w niestandardowym pakiecie instalacyjnym. Tworząc niestandardowy pakiet instalacyjny, możesz określić parametry wiersza poleceń, na przykład, aby zainstalować aplikację w trybie cichym.

W celu utworzenia niestandardowego pakietu instalacyjnego:

1. W drzewie konsoli wybierz **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Nad listą pakietów instalacyjnych kliknij przycisk **Utwórz pakiet instalacyjny**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

3. W pierwszym kroku kreatora wybierz **Utwórz pakiet instalacyjny dla określonego pliku wykonywalnego**.

4. W kolejnym kroku kreatora określ nazwę niestandardowego pakietu instalacyjnego.

5. W kolejnym kroku kreatora kliknij przycisk **Przeglądaj** i w standardowym oknie **Otwórz** systemu Windows wybierz plik archiwum znajdujący się na dostępnych dyskach w celu utworzenia niestandardowego pakietu instalacyjnego.

   Możesz przesłać archiwum ZIP, CAB, TAR lub TAR.GZ. Nie jest możliwe utworzenie pakietu instalacyjnego z pliku SFX (samorozpakowujące się archiwum).

   Pliki są pobierane na Serwer administracyjny Kaspersky Security Center.

6. W kolejnym kroku kreatora określ parametry wiersza poleceń pliku wykonywalnego.

   Możesz określić parametry wiersza poleceń, aby zainstalować aplikację z pakietu instalacyjnego w trybie cichym. Określanie parametrów wiersza poleceń jest opcjonalne.

   Jeśli chcesz, skonfiguruj następujące opcje:

- **Kopiuj całą zawartość folderu do pakietu instalacyjnego**

  Wybierz tę opcję, jeśli plikowi wykonywalnemu towarzyszą dodatkowe pliki wymagane do zainstalowania aplikacji. Przed włączeniem tej opcji upewnij się, że wszystkie wymagane pliki są przechowywane w tym samym folderze. Jeśli ta opcja jest włączona, aplikacja doda całą zawartość folderu, w tym określony plik wykonywalny, do pakietu instalacyjnego.

- **Konwertuj ustawienia na zalecane wartości dla aplikacji rozpoznawanych przez Kaspersky Security Center**

  Aplikacja zostanie zainstalowana z zalecanymi ustawieniami, jeśli informacje o określonej aplikacji znajdują się w bazie danych Kaspersky.

  Jeśli wprowadziłeś parametry w polu **Wiersz polecenia pliku wykonywalnego**, zostaną zapisane z zalecanymi ustawieniami.

  Domyślnie opcja ta jest włączona.

  Baza danych Kaspersky jest tworzona i zarządzana przez analityków z Kaspersky. Dla każdej aplikacji dodanej do bazy danych analitycy z Kaspersky definiują optymalne ustawienia instalacji. Ustawienia są definiowane, aby zapewnić pomyślną zdalną instalację aplikacji na urządzeniu klienckim. Baza danych jest automatycznie aktualizowana na Serwerze administracyjnym, gdy uruchamiasz zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego.

Zostanie uruchomiony proces tworzenia niestandardowego pakietu instalacyjnego.

Kreator informuje, gdy proces zostanie zakończony.

Jeśli niestandardowy pakiet instalacyjny nie zostanie utworzony, zostanie wyświetlona odpowiednia wiadomość.

7. W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

Pakiet instalacyjny, który utworzyłeś, zostanie pobrany do podfolderu Packages folderu współdzielonego Serwera administracyjnego. Po pobraniu, niestandardowy pakiet instalacyjny pojawi się na liście pakietów instalacyjnych.

Na liście pakietów instalacyjnych na Serwerze administracyjnym możesz przejrzeć i edytować właściwości niestandardowego pakietu instalacyjnego.

Przeglądanie i edytowanie właściwości niestandardowych pakietów instalacyjnych

Po utworzeniu niestandardowego pakietu instalacyjnego, możesz przejrzeć ogólne informacje o pakiecie instalacyjnym i określić ustawienia instalacyjne w oknie właściwości.

W celu przejrzenia i edytowania właściwości niestandardowego pakietu instalacyjnego:

1. W drzewie konsoli wybierz **Serwer administracyjny → Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Z menu kontekstowego pakietu instalacyjnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości wybranego pakietu instalacyjnego.

3. Przejrzyj następujące informacje:

- Nazwa pakietu instalacyjnego
- Nazwa aplikacji spakowanej w niestandardowy pakiet instalacyjny
- Wersja aplikacji
- Data utworzenia pakietu instalacyjnego
- Ścieżka do niestandardowego pakietu instalacyjnego na Serwerze administracyjnym
- Parametry wiersza polecenia pliku wykonywalnego

4. Określ następujące ustawienia:
   - Nazwa pakietu instalacyjnego
   - **Zainstaluj wymagane ogólne składniki systemu**

     Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

     Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

     Domyślnie opcja ta jest wyłączona.

     Ta opcja jest dostępna tylko, gdy aplikacja dodana do pakietu instalacyjnego zostanie rozpoznana przez Kaspersky Security Center.

   - **Wiersz polecenia pliku wykonywalnego**

     Jeśli dla cichej instalacji aplikacja wymaga dodatkowych parametrów, określ je w tym polu. Więcej informacji można znaleźć w dokumentacji producenta.

     Możesz też wprowadzić inne parametry.

     Ta opcja jest dostępna tylko dla pakietów, które nie są tworzone w oparciu o aplikacje Kaspersky.

5. Kliknij przycisk **OK** lub **Zastosuj**, aby zapisać zmiany (jeśli jakiekolwiek są).

Nowe ustawienia zostaną zapisane.

Uzyskiwanie pakietu instalacyjnego Agenta sieciowego z pakietu dystrybucyjnego Kaspersky Security Center

Pakiet instalacyjny Agenta sieciowego można uzyskać z pakietu dystrybucyjnego Kaspersky Security Center bez konieczności instalowania Kaspersky Security Center. Następnie możesz użyć pakietu instalacyjnego do zainstalowania Agenta sieciowego na urządzeniach klienckich.

W celu uzyskania pakietu instalacyjnego Agenta sieciowego z pakietu dystrybucyjnego Kaspersky Security Center:

1. Uruchom plik wykonywalny ksc_<numer wersji>.<numer kompilacji> _full_<język lokalizacji>.exe z pakietu dystrybucyjnego Kaspersky Security Center.
2. W otwartym oknie kliknij odnośnik **Wyodrębnij pakiety instalacyjne**.
3. Na liście pakietów instalacyjnych zaznacz pole obok pakietu instalacyjnego Agenta sieciowego, a następnie kliknij przycisk **Dalej**.
4. W razie potrzeby kliknij przycisk **Przeglądaj**, aby zmienić wyświetlany folder, do którego ma zostać wypakowany pakiet instalacyjny.
5. Kliknij przycisk **Wyodrębnij**.

   Aplikacja rozpakowuje pakiet instalacyjny Agenta sieciowego.
6. Po zakończeniu procesu kliknij przycisk **Zamknij**.

Pakiet instalacyjny Agenta sieciowego zostanie rozpakowany do wybranego folderu.

Możesz użyć pakietu instalacyjnego do zainstalowania Agenta sieciowego na jeden z następujących sposobów:

- Lokalnie, uruchamiając plik setup.exe z wyodrębnionego folderu
- Przez cichą instalację
- Korzystając z zasad grupy Microsoft Windows

Rozsyłanie pakietów instalacyjnych na podrzędne Serwery administracyjne

W celu rozesłania pakietów instalacyjnych na podrzędne Serwery administracyjne:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie podrzędne Serwery administracyjne.
2. Utwórz zadanie rozsyłania pakietu instalacyjnego na podrzędne Serwery administracyjne w jeden z następujących sposobów:

   - Jeśli chcesz utworzyć zadanie dla podrzędnych Serwerów administracyjnych w wybranej grupie administracyjnej, uruchom tworzenie grupowego zadania dla tej grupy.
   - Jeśli chcesz utworzyć zadanie dla określonych podrzędnych Serwerów administracyjnych, uruchom tworzenie zadania dla określonych urządzeń.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania, w węźle **Serwer administracyjny Kaspersky Security Center**, w folderze **Zaawansowane** wybierz **Rozsyłanie pakietu instalacyjnego** jako typ zadania.

   Kreator tworzenia nowego zadania utworzy zadanie rozsyłania wybranych pakietów instalacyjnych na określone podrzędne Serwery administracyjne.
3. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Wybrane pakiety instalacyjne zostaną skopiowane na określone podrzędne Serwery administracyjne.

Rozsyłanie pakietów instalacyjnych poprzez punkty dystrybucji

Do rozesłania pakietów instalacyjnych w obrębie grupy administracyjnej można wykorzystać punkty dystrybucji.

Po odebraniu pakietów instalacyjnych z Serwera administracyjnego, punkty dystrybucji automatycznie rozsyłają je na urządzenia klienckie, korzystając z multiemisji IP. Rozsyłanie nowych pakietów instalacyjnych w obrębie grupy administracyjnej przy użyciu multiemisji IP występuje tylko raz. Jeśli w momencie dystrybucji pakietów urządzenie klienckie było odłączone od sieci korporacyjnej, wówczas Agent sieciowy (na urządzeniu klienckim) automatycznie pobierze potrzebny pakiet instalacyjny z punktu dystrybucji po uruchomieniu zadania instalacji.

Przesyłanie rezultatów instalacji aplikacji do Kaspersky Security Center

Po utworzeniu pakietu instalacyjnego aplikacji możesz skonfigurować go tak, aby wszystkie informacje diagnostyczne dotyczące wyników instalacji aplikacji były przesyłane do Kaspersky Security Center. Dla pakietów instalacyjnych aplikacji firmy Kaspersky przesyłanie informacji diagnostycznych o wynikach instalacji aplikacji jest skonfigurowane domyślnie i nie jest konieczna dodatkowa konfiguracja.

W celu skonfigurowania przesyłania informacji diagnostycznych dotyczących wyników instalacji aplikacji do Kaspersky Security Center:

1. Przejdź do folderu z pakietem instalacyjnym utworzonym dla wybranej aplikacji przy użyciu Kaspersky Security Center. Folder można znaleźć w folderze współdzielonym wskazanym podczas instalacji Kaspersky Security Center.

2. Otwórz plik z rozszerzeniem .kpd lub .kud w programie umożliwiającym jego edycję (na przykład w notatniku systemu Microsoft Windows).

   Plik będzie miał format typowego pliku konfiguracyjnego .ini.

3. Dodaj do pliku następujące wiersze:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Polecenie to konfiguruje Kaspersky Security Center tak, aby program czekał na zakończenie instalacji aplikacji, dla której tworzony jest pakiet instalacyjny oraz na analizę kodu zwrotnego instalatora. Jeśli chcesz wyłączyć przesyłanie danych diagnostycznych, ustaw wartość klucza Wait na 0.

4. Dodaj opis kodów zwrotnych w celu pomyślnego zakończenia instalacji. W tym celu, do pliku dodaj następujące wiersze:

   ```
   [SetupProcessResult_SuccessCodes]
   <kod zwrotny>=[<opis>]
   <kod zwrotny 1>=[<opis>]
   ...
   ```

   W nawiasach kwadratowych znajdują się opcjonalne klucze.

   Składnia dla wierszy:

- `<kod zwrotny>`. Dowolna liczba odpowiadająca kodowi zwrotnemu instalatora. Można podać dowolną liczbę kodów zwrotnych.

- `<opis>`. Opis tekstowy wyniku instalacji. Opis można pominąć.

5. Dodaj opis kodów zwrotnych dla instalacji zakończonej niepowodzeniem. W tym celu, do pliku dodaj następujące wiersze:

   ```
   [SetupProcessResult_ErrorCodes]
   <kod zwrotny>=[<opis>]
   <kod zwrotny 1>=[<opis>]
   ...
   ```

   Składnia tych wierszy jest identyczna jak składnia wierszy zawierających kody zwrotne instalacji zakończonej powodzeniem.

6. Zapisz wszystkie zmiany i zamknij plik .kpd lub .kud.

Wyniki instalacji aplikacji określonej przez użytkownika zostaną zapisane w raportach programu Kaspersky Security Center i pojawią się na liście zdarzeń, w raportach i dziennikach wykonywania zadań.

Definiowanie adresu serwera proxy KSN pod kątem pakietów instalacyjnych

W przypadku zmiany adresu lub domeny Serwera administracyjnego, możesz zdefiniować adres serwera proxy KSN dla pakietu instalacyjnego.

W celu zdefiniowania adresu serwera proxy KSN dla pakietu instalacyjnego:

1. W drzewie konsoli, w folderze **Zdalna instalacja**, kliknij dwukrotnie podfolder **Pakiety instalacyjne**.

2. W otwartym menu wybierz **Właściwości**.

3. W otwartym oknie właściwości wybierz podsekcję **Ogólne**.

4. W podsekcji **Ogólne** okna właściwości wprowadź adres serwera proxy KSN.

Pakiety instalacyjne będą używać tego adresu domyślnie.

Pobieranie aktualnych wersji aplikacji

Kaspersky Security Center pozwala na pobieranie aktualnych wersji aplikacji korporacyjnych przechowywanych na serwerach Kaspersky.

W celu pobrania aktualnych wersji aplikacji korporacyjnych firmy Kaspersky:

1. Wykonaj jedną z poniższych czynności:

   - W drzewie konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego, upewnij się, że zakładka **Monitorowanie** jest wybrana, a w sekcji **Wdrażanie** kliknij odnośnik **Dostępne są nowe wersje produktów Kaspersky**.

Odnośnik **Dostępne są nowe wersje produktów Kaspersky** stanie się widoczny, gdy Serwer administracyjny odnajdzie nową wersję aplikacji korporacyjnej na serwerze Kaspersky.

- W drzewie konsoli wybierz **Zaawansowane → Zdalna instalacja → Pakiety instalacyjne**, a w obszarze roboczym kliknij **Akcje dodatkowe** i z listy rozwijalnej wybierz **Wyświetl aktualne wersje aplikacji Kaspersky**.

Zostanie wyświetlona lista bieżących wersji aplikacji Kaspersky.

2. Możesz filtrować listę aplikacji Kaspersky, aby uprościć wyszukiwanie wymaganej aplikacji.

   W górnej części okna **Aktualne wersje aplikacji** kliknij odnośnik **Filtr**, aby przefiltrować listę aplikacji według następujących kryteriów:

   - **Komponenty**. Użyj tego kryterium, aby przefiltrować listę aplikacji Kaspersky według obszarów ochrony używanych w Twojej sieci.
   - **Typ pobieranego oprogramowania**. Użyj tego kryterium, aby przefiltrować listę aplikacji Kaspersky według typu aplikacji.
   - **Wyświetlane oprogramowanie i aktualizacje**. Użyj tego kryterium, aby wyświetlić dostępne aplikacje firmy Kaspersky według określonych wersji.
   - **Wyświetlane wersje językowe oprogramowania i aktualizacji**. Użyj tego kryterium, aby wyświetlić aplikacje Kaspersky z określonym językiem lokalizacji.

   Kliknij przycisk **Zastosuj**, aby zastosować wybrane filtry.

3. Z listy wybierz żądaną aplikację.

4. Pobierz pakiet dystrybucyjny aplikacji, klikając odnośnik w wierszu **Adres internetowy pakietu dystrybucyjnego**.

Aktualizacje zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center. Jeśli ta wersja jest nowsza niż aktualna wersja, te aktualizacje są wyświetlane, ale nie można ich zatwierdzić. Ponadto żadne pakiety instalacyjne nie mogą być tworzone z takich aktualizacji, dopóki nie zaktualizujesz Kaspersky Security Center. Zostaniesz poproszony o uaktualnienie instancji Kaspersky Security Center do wymaganej wersji minimalnej.

Jeżeli dla wybranej aplikacji wyświetlony jest przycisk **Pobierz aplikacje i utwórz pakiety instalacyjne**, możesz go kliknąć w celu automatycznego pobrania pakietu dystrybucyjnego aplikacji i utworzenia pakietu instalacyjnego. Kaspersky Security Center pobierze pakiet dystrybucyjny aplikacji na Serwer administracyjny, do folderu współdzielonego określonego w trakcie instalacji Kaspersky Security Center. Automatycznie utworzony pakiet instalacyjny jest wyświetlany w drzewie konsoli, w folderze **Zdalna instalacja**, w podfolderze **Pakiety instalacyjne**.

Po zamknięciu okna **Aktualne wersje aplikacji**, odnośnik **Dostępne są nowe wersje produktów Kaspersky** znika z sekcji **Wdrażanie**.

Możesz utworzyć pakiety instalacyjne dla nowych wersji aplikacji i zarządzać nowo utworzonymi pakietami instalacyjnymi w drzewie konsoli, w folderze **Zdalna instalacja**, podfolderze **Pakiety instalacyjne**.

Możesz także otworzyć okno **Aktualne wersje aplikacji**, klikając odnośnik **Wyświetl aktualne wersje aplikacji Kaspersky** w obszarze roboczym folderu **Pakiety instalacyjne**.

Przygotowywanie urządzenia do zdalnej instalacji. Narzędzie riprep.exe

Zdalna instalacja aplikacji na urządzeniu klienckim może zakończyć się błędem z następujących powodów:

- Zadanie to było już wykonane na tym urządzeniu i zakończyło się powodzeniem. W tym przypadku zadanie nie musi być wykonywane ponownie.
- W momencie uruchamiania zadania urządzenie było wyłączone. Należy włączyć urządzenie i ponownie uruchomić zadanie.
- Nie istnieje połączenie między Serwerem administracyjnym a Agentem sieciowym zainstalowanym na urządzeniu klienckim. Aby określić przyczynę wystąpienia tego problemu, użyj narzędzia do zdalnej diagnostyki urządzeń klienckich (klactgui).
- Jeśli na urządzeniu nie ma zainstalowanego Agenta sieciowego, podczas zdalnej instalacji mogą wystąpić następujące problemy:
  - Na urządzeniu klienckim jest włączona opcja **Wyłącz proste udostępnianie plików**.
  - Na urządzeniu klienckim nie jest uruchomiona usługa serwera.
  - Na urządzeniu klienckim zamknięte są wymagane porty.
  - Konto, z poziomu którego wykonywane jest zadanie, ma niewystarczające uprawnienia.

  Aby rozwiązać problemy, które wystąpiły w trakcie instalowania aplikacji na urządzeniu klienckim bez zainstalowanego Agenta sieciowego, możesz użyć narzędzia do przygotowywania urządzeń do zdalnej instalacji (riprep).

Ta sekcja zawiera opis narzędzia pozwalającego na przygotowanie urządzenia do zdalnej instalacji (riprep). Narzędzie znajduje się w folderze instalacyjnym Kaspersky Security Center, na urządzeniu, na którym zainstalowano Serwer administracyjny.

Narzędzie do przygotowywania urządzenia do zdalnej instalacji nie zadziała na systemie Microsoft Windows XP Home Edition.

Przygotowywanie urządzenia do zdalnej instalacji w trybie interaktywnym

W celu przygotowania urządzenia do zdalnej instalacji w trybie interaktywnym:

1. Uruchom plik riprep.exe na urządzeniu klienckim.
2. W oknie głównym narzędzia przygotowującego do zdalnej instalacji wybierz następujące opcje:
   - **Wyłącz proste udostępnianie plików**
   - **Uruchom usługę Serwera administracyjnego**
   - **Otwórz porty**

- **Dodaj konto**
- **Wyłącz kontrolę konta użytkownika (UAC)** (opcja ta jest dostępna tylko dla urządzeń z systemami Microsoft Windows Vista, Microsoft Windows 7 oraz Microsoft Windows Server 2008)

3. Kliknij przycisk **Uruchom**.

   Etapy przygotowywania urządzenia do zdalnej instalacji będą wyświetlane w dolnej części okna głównego narzędzia.

Jeśli zaznaczyłeś opcję **Dodaj konto**, po utworzeniu konta zostanie wyświetlony monit o wprowadzenie nazwy konta i hasła. Spowoduje to utworzenie konta lokalnego należącego do grupy lokalnych administratorów.

Jeśli wybrałeś opcję **Wyłącz kontrolę konta użytkownika (UAC)**, próba wyłączenia Kontroli konta użytkownika zostanie wykonana nawet wtedy, gdy była ona wyłączona przed uruchomieniem narzędzia. Po wyłączeniu Kontroli konta użytkownika, zostaniesz poproszony o ponowne uruchomienie urządzenia.

Przygotowywanie urządzenia do zdalnej instalacji w trybie nieinteraktywnym

W celu przygotowywania urządzenia do zdalnej instalacji w trybie nieinteraktywnym:

Uruchom plik riprep.exe na urządzeniu klienckim z poziomu wiersza poleceń, podając wymagany zestaw przełączników.

Składnia wiersza poleceń narzędzia:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Opisy przełączników:

- `-silent`—uruchamia narzędzie w trybie nieinteraktywnym.
- `-cfg CONFIG_FILE`—określa konfigurację narzędzia, gdzie `CONFIG_FILE` to ścieżka dostępu do pliku konfiguracyjnego (pliku posiadającego rozszerzenie .ini).
- `-tl traceLevel`—określa poziom śledzenia, gdzie `traceLevel` to cyfra od 0 do 5. Jeśli nie określono żadnego przełącznika, używana jest wartość 0.

Uruchamiając narzędzie w trybie cichym, możesz wykonać następujące zadania:

- Wyłączyć proste udostępnianie plików
- Uruchomić usługę serwera na urządzeniu klienckim
- Otworzyć porty
- Utworzyć konto lokalne
- Wyłączyć kontrolę konta użytkownika (UAC)

Możesz określić parametry dla przygotowywania urządzenia do zdalnej instalacji w pliku konfiguracyjnym podanym w przełączniku `-cfg`. W celu zdefiniowania tych parametrów, do pliku konfiguracyjnego należy dodać następujące informacje:

- W sekcji `Common` określ, które zadania mają zostać wykonane:
  - `DisableSFS` — wyłącza proste udostępnianie plików (0—zadanie jest wyłączone; 1—zadanie jest włączone).
  - `StartServer` — uruchamia usługę serwera (0—zadanie jest wyłączone; 1—zadanie jest włączone).
  - `OpenFirewallPorts` — otwiera potrzebne porty (0—zadanie jest wyłączone; 1—zadanie jest włączone).
  - `DisableUAC` — wyłącza Kontrolę konta użytkownika (UAC) (0—zadanie jest wyłączone; 1—zadanie jest włączone).
  - `RebootType` — określa zachowanie w przypadku, gdy konieczne jest ponowne uruchomienie urządzenia, a UAC jest wyłączona. Możesz użyć następujących wartości:
    - 0—nigdy nie uruchamiaj urządzenia ponownie.
    - 1—uruchom urządzenie ponownie, jeśli UAC była włączona przed uruchomieniem narzędzia.
    - 2—wymuś ponowne uruchomienie, jeśli UAC była włączona przed uruchomieniem narzędzia.
    - 4—zawsze uruchamiaj urządzenie ponownie.
    - 5—zawsze wymuszaj ponowne uruchomienie urządzenia.
- W sekcji `UserAccount` określ nazwę konta (`user`) i jego hasło (`Pwd`).

Przykładowa zawartość pliku konfiguracyjnego:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1

[UserAccount]
user=Admin
Pwd=Pass123
```

Po zakończeniu pracy narzędzia, w jego folderze zostaną utworzone następujące pliki:

- riprep.txt—raport z działania, w którym znajdują się wszystkie etapy działania narzędzia wraz z powodami takich działań.
- riprep.log—plik śledzenia (jest on tworzony, gdy poziom śledzenia został ustawiony powyżej 0).

Przygotowanie urządzenia Linux do zdalnej instalacji Agenta sieciowego

W celu przygotowania urządzenia z systemem Linux do zdalnej instalacji Agenta sieciowego:

1. Upewnij się, że następujące oprogramowanie jest zainstalowane na docelowym urządzeniu Linux:
   - Sudo
   - Perl language interpreter wersja 5.10 lub wyższa

2. Przetestuj konfigurację urządzenia:

   a. Sprawdź, czy możesz połączyć się z urządzeniem poprzez klienta SSH (np. PuTTY).

      Jeśli nie możesz połączyć się z urządzeniem, otwórz plik /etc/ssh/sshd_config i upewnij się, że następujące ustawienia posiadają odpowiednie wartości przedstawione poniżej:

      ```
      PasswordAuthentication no
      ```

      ```
      ChallengeResponseAuthentication yes
      ```

      Zapisz plik (jeśli to konieczne) i uruchom ponownie usługę SSH przy pomocy polecenia `sudo service ssh restart`.

   b. Wyłącz hasło do programu sudo dla konta użytkownika, z poziomu którego nawiązywane jest połączenie.

   c. Użyj polecenia `visudo` w sudo, aby otworzyć plik konfiguracyjny sudoers.

      W otwartym pliku znajdź wiersz rozpoczynający się od `%sudo` (lub od `%wheel`, jeśli używasz systemu operacyjnego CentOS). W tym wierszu podaj następujące informacje: < `nazwa użytkownika` > `ALL = (ALL) NOPASSWD: ALL`. W tym przypadku < `username` > to konto użytkownika, które będzie używane do łączenia urządzenia przy użyciu SSH. Jeśli używasz systemu operacyjnego Astra Linux, w pliku /etc/sudoers dodaj ostatni wiersz z następującym tekstem: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Zapisz plik sudoers i zamknij go.

   e. Ponownie nawiąż połączenie z urządzeniem poprzez SSH i upewnij się, że usługa Sudo nie żąda wprowadzenia hasła. Możesz to zrobić, korzystając z polecenia `sudo whoami`.

3. Otwórz plik /etc/systemd/logind.conf, a następnie wykonaj jedną z następujących czynności:

   - Określ 'no' jako wartość dla ustawienia KillUserProcesses: `KillUserProcesses=no`.
   - Dla ustawienia KillExcludeUsers wpisz nazwę użytkownika konta, z poziomu którego zdalna instalacja zostanie uruchomiona, na przykład, `KillExcludeUsers=root`.

   W celu zastosowania zmienionych ustawień uruchom urządzenie Linux ponownie lub wykonaj następujące polecenie:

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

4. Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

5. Pobierz i utwórz pakiet instalacyjny:

   a. Przed zainstalowaniem pakietu na urządzeniu upewnij się, że dla tego pakietu są już zainstalowane wszystkie zależności (programy i biblioteki).

      Dla każdego pakietu można wyświetlić jego zależności, korzystając z narzędzi specyficznych dla dystrybucji Linuksa, na którym ten pakiet ma zostać zainstalowany. Więcej informacji na temat narzędzi można znaleźć w dokumentacji do systemu operacyjnego.

   b. Pobierz pakiet instalacyjny Agenta sieciowego.

   c. W celu utworzenia zdalnego pakietu instalacyjnego użyj następujących plików:

      - klnagent.kpd
      - akinstall.sh

- Pakiet .deb lub .rpm Agenta sieciowego

6. Utwórz zadanie zdalnej instalacji z następującymi ustawieniami:

   - Na stronie **Settings** Kreatora tworzenia nowego zadania zaznacz pole **Using operating system resources through Administration Server**. Odznacz wszystkie pozostałe pola.

   - W oknie **Wybieranie konta do uruchomienia zadania**, aby uruchomić zadanie, określ ustawienia konta użytkownika, które jest używane do łączenia urządzenia poprzez SSH.

7. Uruchom zadanie zdalnej instalacji. Użyj opcji polecenia `su`, aby zachować środowisko: `-m, -p, --preserve-environment`.

Może zostać zwrócony błąd, jeśli instalujesz Agenta sieciowego z SSH na urządzeniach działających pod kontrolą systemu Fedora w wersjach wcześniejszych niż 20. W tym przypadku, aby instalacja Agenta sieciowego zakończyła się pomyślnie, zakomentuj opcję Defaults requiretty (załącz w składni komentarza, aby usunąć z kodu przetwarzania) w pliku /etc/sudoers. Szczegółowy opis warunku opcji Defaults requiretty, która może powodować problemy podczas połączenia SSH, można znaleźć na stronie Bugzilla.

Przygotowanie urządzenia z systemem SUSE Linux Enterprise Server 15 do instalacji Agenta sieciowego

W celu zainstalowania Agenta sieciowego na urządzeniu z systemem operacyjnym SUSE Linux Enterprise Server 15,

przed instalacją Agenta sieciowego uruchom następujące polecenie:

```
$ sudo zypper install insserv-compat
```

To umożliwia zainstalowanie pakietu insserv-compat i poprawne skonfigurowanie Agenta sieciowego.

Uruchom polecenie `rpm -q insserv-compat`, aby sprawdzić, czy pakiet jest już zainstalowany.

Jeśli Twoja sieć obejmuje wiele urządzeń z systemem SUSE Linux Enterprise Server 15, możesz użyć specjalnego oprogramowania do konfigurowania i zarządzania infrastrukturą firmy. Korzystając z tego oprogramowania, możesz automatycznie zainstalować pakiet insserv-compat na wszystkich niezbędnych urządzeniach jednocześnie. Na przykład, możesz użyć Puppet, Ansible, Chef lub możesz utworzyć własny skrypt — użyj dowolnej wygodnej dla siebie metody.

Oprócz instalacji pakietu insserv-compat, upewnij się, że całkowicie przygotowałeś swoje urządzenia z systemem Linux. Następnie, wdróż i zainstaluj Agenta sieciowego.

Przygotowanie urządzenia macOS do zdalnej instalacji Agenta sieciowego

W celu przygotowania urządzenia z systemem macOS do zdalnej instalacji Agenta sieciowego:

1. Upewnij się, że narzędzie sudo jest zainstalowane na docelowym urządzeniu macOS.

2. Przetestuj konfigurację urządzenia:

   a. Upewnij się, że port 22 jest otwarty na urządzeniu klienckim. Aby to zrobić w **Preferencjach systemowych** otwórz panel **Udostępnianie** i upewnij się, że pole **Zdalne logowanie** jest zaznaczone.

Możesz połączyć się z urządzeniem klienckim przez Secure Shell (SSH) tylko przez port 22. Nie można zmienić numeru portu.

Możesz użyć polecenia `ssh <nazwa_urządzenia>`, aby zdalnie zalogować się na urządzenie macOS. W panelu **Udostępnianie** możesz użyć opcji **Zezwalaj na dostęp przez**, aby określić zakres użytkowników, którzy mogą uzyskać dostęp do urządzenia macOS.

b. Wyłącz hasło do programu sudo dla konta użytkownika, z poziomu którego nawiązywane jest połączenie.

Użyj polecenia `sudo visudo` w Terminalu, aby otworzyć plik konfiguracyjny sudoers. W otwartym pliku, we wpisie `User privilege specification` określ następujące elementy: `username ALL = (ALL) NOPASSWD: ALL`. W tym przypadku `username` to konto użytkownika, które będzie używane do łączenia urządzenia przy użyciu SSH.

c. Zapisz plik sudoers i zamknij go.

d. Ponownie nawiąż połączenie z urządzeniem poprzez SSH i upewnij się, że usługa Sudo nie żąda wprowadzenia hasła. Możesz to zrobić, korzystając z polecenia `sudo whoami`.

3. Pobierz i utwórz pakiet instalacyjny:

a. Pobierz pakiet instalacyjny Agenta sieciowego, korzystając z jednej z następujących metod:

- W drzewie konsoli, otwierając menu kontekstowe na **Zdalna instalacja** → **Pakiety instalacyjne** i wybierając **Pokaż aktualne wersje aplikacji**, aby wybrać z dostępnych pakietów
- Pobierając odpowiednią wersję Agenta sieciowego ze strony internetowej pomocy technicznej: https://support.kaspersky.com/pl
- Prosząc specjalistów z pomocy technicznej o pakiet

b. W celu utworzenia zdalnego pakietu instalacyjnego użyj następujących plików:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. Utwórz zadanie zdalnej instalacji z następującymi ustawieniami:

- Na stronie **Ustawienia** Kreatora tworzenia nowego zadania zaznacz pole **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**. Odznacz wszystkie pozostałe pola.
- Na stronie **Wybieranie konta do uruchomienia zadania** określ ustawienia konta użytkownika, które jest używane do łączenia urządzenia poprzez SSH.

Urządzenie klienckie jest gotowe do zdalnej instalacji Agenta sieciowego za pośrednictwem odpowiedniego zadania, które utworzyłeś.

Aplikacje Kaspersky: licencjonowanie i aktywacja

Ta sekcja opisuje funkcje Kaspersky Security Center związane z pracą z kluczami licencyjnymi dla zarządzanych aplikacji Kaspersky.

Kaspersky Security Center pozwala na wykonywanie scentralizowanego rozsyłania kluczy licencyjnych dla aplikacji Kaspersky na urządzenia klienckie, monitorowanie ich wykorzystania i odnawianie licencji.

Dodając klucz licencyjny przy pomocy Kaspersky Security Center, jego ustawienia są zapisywane na Serwerze administracyjnym. W oparciu o te informacje, aplikacja generuje raport użycia klucza licencyjnego i powiadamia administratora o wygaśnięciu licencji oraz naruszeniu ograniczeń licencyjnych, określonych we właściwościach kluczy licencyjnych. Możesz skonfigurować powiadomienia związane z korzystaniem z kluczy licencyjnych w ustawieniach Serwera administracyjnego.

Licencjonowanie zarządzanych aplikacji

Aplikacje Kaspersky, zainstalowane na zarządzanych urządzeniach, muszą być licencjonowane poprzez zastosowanie pliku klucza lub kodu aktywacyjnego do każdej z aplikacji. Plik klucza lub kod aktywacyjny może zostać rozesłany w następujące sposoby:

- Automatyczne rozsyłanie
- Pakiet instalacyjny zarządzanej aplikacji
- Zadanie *Dodaj klucz licencyjny* dla zarządzanej aplikacji
- Ręczna aktywacja zarządzaną aplikacją

Możesz dodać nowy aktywny lub zapasowy klucz licencyjny za pomocą dowolnej z metod wymienionych powyżej. Aplikacja firmy Kaspersky używa w danej chwili aktywnego klucza i przechowuje zapasowy klucz do zastosowania po wygaśnięciu aktywnego klucza. Aplikacja, dla której dodajesz klucz licencyjny, określa, czy klucz jest aktywny, czy zapasowy. Definicja klucza nie zależy od metody użytej do dodania nowego klucza licencyjnego.

Automatyczne rozsyłanie

Jeśli używasz różnych zarządzanych aplikacji i musisz rozesłać określony plik klucza lub kod aktywacyjny na urządzenia, zdecyduj się na inne sposoby wdrożenia tego kodu aktywacyjnego lub pliku klucza.

Kaspersky Security Center umożliwia automatyczne rozesłanie dostępnych kluczy licencyjnych na urządzenia. Na przykład, trzy klucze licencyjne są przechowywane w repozytorium Serwera administracyjnego. Zaznaczyłeś pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** dla wszystkich trzech kluczy licencyjnych. Aplikacja zabezpieczająca Kaspersky—na przykład Kaspersky Endpoint Security for Windows—jest zainstalowana na urządzeniach w organizacji. Zostanie wykryte nowe urządzenie, do którego musi być rozesłany klucz licencyjny. Aplikacja określi, na przykład, że na urządzenie mogą zostać rozesłane dwa klucze licencyjne z repozytorium: klucz licencyjny o nazwie *Key_1* oraz klucz licencyjny o nazwie *Key_2*. Jeden z tych kluczy licencyjnych zostanie zastosowany na urządzeniu. W tym przypadku nie można przewidzieć, który z dwóch kluczy licencyjnych zostanie rozesłany na urządzenie, ponieważ automatyczne rozesłanie kluczy licencyjnych nie oferuje administratorowi podejmowania żadnych działań.

Podczas rozsyłania klucza licencyjnego urządzenia są zliczane dla tego klucza licencyjnego. Musisz upewnić się, że liczba urządzeń, na których klucz licencyjny został zastosowany, nie przekracza limitu określonego przez licencję. Jeśli liczba urządzeń przekracza limit określony przez licencję, wszystkie urządzenia, które nie zostały objęte licencją, otrzymają stan *Krytyczny*.

Przed zdalną instalacją, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Automatyczne rozsyłanie kluczy licencyjnych

  lub
- Kaspersky Security Center Web Console:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Automatyczne rozsyłanie kluczy licencyjnych

Dodawanie pliku klucza lub kodu aktywacyjnego do pakietu instalacyjnego zarządzanej aplikacji

Z powodów bezpieczeństwa, ta opcja nie jest zalecana. Plik klucza lub kod aktywacyjny dodane do pakietu instalacyjnego mogą być zagrożone.

Jeśli instalujesz zarządzaną aplikację przy użyciu pakietu instalacyjnego, możesz określić kod aktywacyjny lub plik klucza w tym pakiecie instalacyjnym lub w zasadzie aplikacji. Klucz licencyjny zostanie rozesłany na zarządzane urządzenia podczas kolejnej synchronizacji urządzenia z Serwerem administracyjnym.

Dostępne instrukcje:

- Konsola administracyjna:
  - Tworzenie pakietu instalacyjnego
  - Instalowanie aplikacji na urządzeniach klienckich

  lub
- Kaspersky Security Center Web Console: Dodawanie klucza licencyjnego do pakietu instalacyjnego

Rozesłanie poprzez zadanie Dodaj klucz licencyjny dla zarządzanej aplikacji

Jeśli zdecydujesz się na użycie zadania *Dodaj klucz licencyjny* dla zarządzanej aplikacji, możesz wybrać klucz licencyjny, który musi zostać rozesłany na urządzenia, oraz wybrać urządzenia w dowolny sposób—na przykład, wybierając grupę administracyjną lub wybór urządzeń.

Przed zdalną instalacją, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego

- Rozsyłanie klucza licencyjnego na urządzenia klienckie

lub

- Kaspersky Security Center Web Console:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Rozsyłanie klucza licencyjnego na urządzenia klienckie

Ręczne dodawanie kodu aktywacyjnego lub pliku klucza do urządzeń

Możesz aktywować zainstalowaną aplikację Kaspersky lokalnie, przy użyciu narzędzi dostępnych w interfejsie aplikacji. Więcej informacji można znaleźć w dokumentacji dla zainstalowanej aplikacji.

Wyświetlanie informacji o używanych kluczach licencyjnych

W celu wyświetlenia informacji o używanych kluczach licencyjnych:

Z drzewa konsoli wybierz folder **Licencje Kaspersky**.

Obszar roboczy folderu wyświetli listę kluczy licencyjnych wykorzystywanych na urządzeniach klienckich.

Obok każdego z kluczy licencyjnych wyświetlana jest ikona odpowiadająca typowi użycia:

-  — informacja o aktualnie używanym kluczu licencyjnym jest uzyskiwana z urządzenia klienckiego podłączonego do Serwera administracyjnego. Plik tego klucza licencyjnego jest przechowywany poza Serwerem administracyjnym.
-  — klucz licencyjny jest przechowywany w repozytorium Serwera administracyjnego. Automatyczne rozsyłanie jest wyłączone dla tego klucza licencyjnego.
-  — klucz licencyjny jest przechowywany w repozytorium Serwera administracyjnego. Automatyczne rozsyłanie jest włączone dla tego klucza licencyjnego.

Możesz wyświetlić informacje dotyczące kluczy licencyjnych używanych do aktywacji aplikacji na urządzeniu klienckim, otwierając sekcję **Aplikacje** okna właściwości urządzenia klienckiego.

Aby określić aktualne ustawienia kluczy licencyjnych wirtualnego Serwera administracyjnego, Serwer administracyjny wysyła żądanie do serwerów aktywacji Kaspersky przynajmniej raz dziennie. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego

W celu dodania klucza licencyjnego do repozytorium Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Licencje Kaspersky**.

2. Uruchom zadanie dodawania kluczy licencyjnych w jeden z następujących sposobów:

   - Z menu kontekstowego listy kluczy licencyjnych wybierz **Dodaj kod aktywacyjny lub plik klucza**.
   - Kliknij odnośnik **Dodaj kod aktywacyjny lub plik klucza**, dostępny w obszarze roboczym listy kluczy licencyjnych.
   - Kliknij przycisk **Dodaj kod aktywacyjny lub plik klucza**.

   Zostanie uruchomiony kreator Kreator dodawania klucza licencyjnego.

3. Wybierz sposób aktywacji Serwera administracyjnego: przy użyciu kodu aktywacyjnego lub przy użyciu pliku klucza.

4. Określ kod aktywacyjny lub plik klucza.

5. Wybierz opcję **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**, jeśli chcesz natychmiast rozesłać odpowiedni klucz licencyjny w swojej sieci. Jeśli nie wybierzesz tej opcji, możesz ręcznie rozpowszechniać klucz licencyjny później.

   W rezultacie plik klucza jest pobierany, a działanie Kreator dodawania klucza licencyjnego zakończone. Teraz dodany klucz licencyjny można znaleźć na liście licencji Kaspersky.

Usuwanie klucza licencyjnego z Serwera administracyjnego

W celu usunięcia klucza licencyjnego z Serwera administracyjnego:

1. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

2. W oknie właściwości Serwera administracyjnego wybierz sekcję **Klucze licencyjne**.

3. Usuń klucz licencyjny, klikając przycisk **Usuń**.

   Klucz licencyjny zostanie usunięty.

Jeśli dodano zapasowy klucz licencyjny, zapasowy klucz licencyjny automatycznie staje się aktywnym kluczem licencyjnym po wcześniejszym usunięciu aktywnego klucza licencyjnego.

Po usunięciu aktywnego klucza licencyjnego Serwera administracyjnego, staną się dostępne funkcje Zarządzanie lukami i poprawkami i Zarządzanie urządzeniami mobilnymi. Możesz ponownie dodać usunięty klucz licencyjny lub dodać nowy klucz licencyjny.

Rozsyłanie klucza licencyjnego na urządzenia klienckie

Kaspersky Security Center pozwala na rozesłanie klucza licencyjnego na urządzenia klienckie przy pomocy zadania rozsyłania klucza licencyjnego.

W celu rozesłania klucza licencyjnego na urządzenia klienckie:

1. Z drzewa konsoli wybierz folder **Licencje Kaspersky**.

2. W obszarze roboczym listy kluczy licencyjnych kliknij przycisk **Automatycznie roześlij klucz licencyjny do zarządzanych urządzeń**.

   Zostanie uruchomiony Kreator tworzenia zadania aktywacji aplikacji. Postępuj zgodnie z instrukcjami kreatora.

Zadania utworzone przy pomocy kreatora tworzenia zadania aktywacji aplikacji dla określonych urządzeń są przechowywane w folderze **Zadania** drzewa konsoli.

Możesz również utworzyć grupowe lub lokalne zadanie rozsyłania klucza licencyjnego przy pomocy Kreatora tworzenia zadania dla grupy administracyjnej i dla urządzenia klienckiego.

Automatyczne rozsyłanie kluczy licencyjnych

Kaspersky Security Center umożliwia automatyczne instalowanie kluczy licencyjnych na zarządzanych urządzeniach, jeśli znajdują się one w repozytorium kluczy licencyjnych na Serwerze administracyjnym.

W celu automatycznego rozsyłania kluczy licencyjnych do zarządzanych urządzeń:

1. Z drzewa konsoli wybierz folder **Licencje Kaspersky**.
2. W obszarze roboczym folderu wybierz klucz licencyjny, który chcesz automatycznie rozesłać na urządzenia.
3. Otwórz okno właściwości wybranego klucza licencyjnego na jeden z następujących sposobów:
   - Z menu kontekstowego klucza licencyjnego wybierz **Właściwości**.
   - Klikając odnośnik **Pokaż właściwości klucza licencyjnego** w oknie z informacjami dla wybranego klucza licencyjnego.
4. W otwartym oknie właściwości klucza licencyjnego zaznacz pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**. Zamknij okno właściwości klucza licencyjnego.

   Klucz licencyjny zostanie automatycznie rozesłany do wszystkich kompatybilnych urządzeń.

Rozsyłanie klucza licencyjnego odbywa się przy pomocy Agenta sieciowego. Dla aplikacji nie są tworzone żadne zadania rozsyłania kluczy licencyjnych.

Podczas automatycznego rozsyłania klucza licencyjnego brane jest pod uwagę ograniczenie licencyjne dotyczące liczby urządzeń (ograniczenie licencyjne jest ustawione we właściwościach klucza licencyjnego). Jeśli ograniczenie licencyjne zostanie osiągnięte, rozesłanie tego klucza licencyjnego na urządzenia zostanie przerwane automatycznie.

Jeśli zaznaczysz pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** w oknie właściwości klucza licencyjnego, klucz licencyjny jest natychmiast rozpowszechniany w Twojej sieci. Jeśli nie wybierzesz tej opcji, możesz ręcznie rozpowszechniać klucz licencyjny później.

Tworzenie i przeglądanie raportu użycia klucza licencyjnego

W celu utworzenia raportu z wykorzystania kluczy licencyjnych na urządzeniach klienckich:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Wybierz szablon raportu o nazwie **Raport użycia klucza licencyjnego** lub utwórz nowy szablon raportu tego samego typu.

Obszar roboczy raportu użycia klucza licencyjnego wyświetli informacje o aktywnych i zapasowych kluczach licencyjnych używanych na urządzeniach klienckich. Raport zawiera również informacje o urządzeniach, na których używane są klucze licencyjne, oraz o ograniczeniach określonych we właściwościach tych kluczy licencyjnych.

Przeglądanie informacji o kluczach licencyjnych aplikacji

W celu sprawdzenia, jakie klucze licencyjne są używane w aplikacji Kaspersky:

1. W drzewie konsoli Kaspersky Security Center wybierz węzeł **Zarządzane urządzenia** i przejdź na zakładkę **Urządzenia**.
2. Kliknij żądane urządzenie prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.
3. W otwartym oknie właściwości urządzenia wybierz sekcję **Aplikacje**.
4. Na liście aplikacji, która zostanie wyświetlona, wybierz aplikację, której klucze licencyjne chcesz przejrzeć, i kliknij przycisk **Właściwości**.
5. W oknie właściwości aplikacji wybierz sekcję **Klucze licencyjne**.

   Informacje są wyświetlane w obszarze roboczym tej sekcji.

Konfigurowanie ochrony sieci

Ta sekcja zawiera informacje o ręcznej konfiguracji zasad i zadań, informacje o rolach użytkownika, informacje o tworzeniu struktury grupy administracyjnej oraz hierarchii zadań.

Scenariusz: Konfigurowanie ochrony sieci

Kreator wstępnej konfiguracji tworzy zasady i zadania z domyślnymi ustawieniami. Te ustawienia mogą okazać się nieoptymalne lub nawet niedopuszczalne przez organizację. Dlatego zalecane jest dostrojenie tych profili i zadań oraz utworzenie innych profili i zadań, jeśli są konieczne w Twojej sieci.

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Zainstalowano Serwer administracyjny Kaspersky Security Center
- Zainstalowano Kaspersky Security Center Web Console (opcjonalne)

- Zakończyłeś główny scenariusz instalacji Kaspersky Security Center
- Zakończono działanie kreatora wstępnej konfiguracji lub ręcznie utworzono następujące zasady i zadania w grupie administracyjnej **Zarządzane urządzenia**:
  - Profil Kaspersky Endpoint Security
  - Grupowe zadanie aktualizacji Kaspersky Endpoint Security
  - Profil Agenta sieciowego
  - Zadanie *Wyszukiwania luk i wymaganych aktualizacji*

Konfigurowanie ochrony sieci odbywa się w etapach:

1. **Konfiguracja i przesyłanie profili i profili zasad aplikacji firmy Kaspersky**

   Aby skonfigurować i przesłać ustawienia dla aplikacji Kaspersky, zainstalowanych na zarządzanych urządzeniach, możesz użyć dwóch różnych metod zarządzania ochroną—skoncentrowaną na urządzeniu lub skoncentrowaną na użytkowniku. Te dwie metody można także połączyć. Aby zaimplementować zarządzanie ochroną skoncentrowaną na urządzeniu, możesz użyć narzędzi dostarczonych w Konsoli administracyjnej opartej na Microsoft Management Console lub Kaspersky Security Center Web Console. Zarządzanie ochroną skoncentrowaną na użytkowniku może zostać zaimplementowane tylko poprzez Kaspersky Security Center Web Console.

2. **Konfigurowanie zadań zdalnego zarządzania aplikacjami firmy Kaspersky**

   Sprawdź zadania utworzone przy pomocy kreatora wstępnej konfiguracji i dostosuj je (jeśli to konieczne).

   Dostępne instrukcje:

   - Konsola administracyjna:
     - Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security
     - Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console:
     - Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security
     - Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

   Jeśli to konieczne, utwórz dodatkowe zadania do zarządzania aplikacjami firmy Kaspersky, zainstalowanymi na urządzeniach klienckich.

3. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Dostępne instrukcje:

   - Konsola administracyjna: Konfigurowanie maksymalnej liczby zdarzeń
   - Kaspersky Security Center Web Console: Konfigurowanie maksymalnej liczby zdarzeń

Wyniki

Po zakończeniu tego scenariusza, Twoja sieć będzie chroniona przez konfigurację aplikacji Kaspersky, zadania i zdarzenia otrzymane przez Serwer administracyjny:

- Aplikacje firmy Kaspersky są konfigurowane zgodnie z zasadami i profilami zasad.
- Aplikacje są zarządzane za pośrednictwem zestawu zadań.
- Maksymalna liczba zdarzeń, jaka może być przechowywana w bazie danych, została ustawiona.

Jeśli konfiguracja ochrony sieci zostanie zakończona, możesz przejść do konfigurowania regularnych aktualizacji baz danych i aplikacji Kaspersky.

Więcej informacji o sposobie konfiguracji automatycznych odpowiedzi na zagrożenia wykryte przez Kaspersky Sandbox można znaleźć w pomocy online Kaspersky Sandbox 2.0.

Konfiguracja i przydzielanie profili: Metoda skoncentrowana na urządzeniu

Po zakończeniu tego scenariusza, aplikacje zostaną skonfigurowane na wszystkich zarządzanych urządzeniach zgodnie z profilami i profilami zasad aplikacji, które określiłeś.

Wymagania wstępne

Przed rozpoczęciem konfiguracji upewnij się, że zainstalowano Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center Web Console (opcjonalnie). Jeśli zainstalowano Kaspersky Security Center Web Console, możesz wziąć pod uwagę zarządzania ochroną skoncentrowaną na użytkowniku jako alternatywę lub dodatkową opcję dla metody skoncentrowanej na urządzeniu.

Etapy

Scenariusz skoncentrowanego na urządzeniu zarządzania aplikacjami Kaspersky obejmuje następujące kroki:

1. **Konfigurowanie profili aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie profilu dla każdej aplikacji. Zestaw profili zostanie przesłany na urządzenia klienckie.

   Podczas konfigurowania ochrony sieci w kreatorze szybkiego startu Kaspersky Security Center tworzy domyślną politykę dla następujących aplikacji:

   - Kaspersky Endpoint Security for Windows — dla urządzeń klienckich z systemem Windows
   - Kaspersky Endpoint Security for Linux — dla urządzeń klienckich z Linux

   Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowego profilu dla tej aplikacji. Przejdź do ręcznej konfiguracji profilu Kaspersky Endpoint Security.

   Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i potomne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy potomne i podrzędne Serwery administracyjne, aby zabronić wszelkich modyfikacji ustawień skonfigurowanych w nadrzędnej zasadzie. Jeśli chcesz, żeby wymuszone było dziedziczenie tylko części ustawień, możesz zablokować je w profilu nadrzędnym. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w profilach podrzędnych. Utworzona hierarchia profili umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

Dostępne instrukcje:

- Konsola administracyjna: Tworzenie profilu
- Kaspersky Security Center Web Console: Tworzenie profilu

2. **Tworzenie profili zasad (opcjonalnie)**

   Jeśli chcesz, żeby urządzenia w jednej grupie administracyjnej były uruchamiane z różnymi ustawieniami profilu, utwórz profile zasad dla tych urządzeń. Profil zasad jest to inaczej podzbiór ustawień profilu. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z profilem i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowego" profilu, który jest aktywny na zarządzanym urządzeniu.

   Korzystając z warunków aktywacji profilu, możesz zastosować różne profile zasad, na przykład, do urządzeń znajdujących się w określonej jednostce lub grupie bezpieczeństwa Active Directory, posiadającej określoną konfigurację sprzętową lub oznaczoną określonymi znacznikami. Użyj znaczników do filtrowania urządzeń, które spełniają określone kryteria. Na przykład, możesz utworzyć znacznik nazwany *Windows*, oznaczyć tym znacznikiem wszystkie urządzenia działające pod kontrolą systemu operacyjnego Windows, a następnie określić ten znacznik jako warunek aktywacji profilu zasad. W wyniku tego działania, aplikacje Kaspersky zainstalowane na wszystkich urządzeniach działających pod kontrolą systemu Windows będą zarządzane przez swój własny profil zasad.

   Dostępne instrukcje:

   - Konsola administracyjna:
     - Tworzenie profilu zasad
     - Tworzenie reguły aktywacji profilu zasad
   - Kaspersky Security Center Web Console:
     - Tworzenie profilu zasad
     - Tworzenie reguły aktywacji profilu zasad

3. **Przesyłanie profili i profili zasad na zarządzane urządzenia**

   Domyślnie Serwer administracyjny automatycznie synchronizuje się z zarządzanymi urządzeniami co 15 minut. Możesz obejść automatyczną synchronizację i ręcznie uruchomić synchronizację przy pomocy polecenia Wymuś synchronizację. Synchronizacja jest również wymuszana po utworzeniu lub zmianie zasady lub profilu zasady. Podczas synchronizacji nowe lub zmienione profile i profile zasad zostają rozesłane na zarządzane urządzenia.

   Jeśli używasz Kaspersky Security Center Web Console, możesz sprawdzić, czy zasady i profile zasad zostały dostarczone na urządzenie. Kaspersky Security Center określa datę i godzinę dostarczenia we właściwościach urządzenia.

   Dostępne instrukcje:

   - Konsola administracyjna: Wymuszona synchronizacja
   - Kaspersky Security Center Web Console: Wymuszona synchronizacja

Wyniki

Po zakończeniu scenariusza skoncentrowanego na urządzeniu, aplikacje Kaspersky są konfigurowane zgodnie z ustawieniami określonymi i przesłanymi poprzez hierarchię profili.

Skonfigurowane profile i profile zasad aplikacji zostaną automatycznie zastosowane do nowych urządzeń dodanych do grup administracyjnych.

Informacje o metodach zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku

Możesz zarządzać ustawieniami zabezpieczeń z poziomu funkcji urządzenia i z poziomu roli użytkownika. Pierwsza metoda nosi nazwę *zarządzanie ochroną skoncentrowaną na urządzeniu*, a druga nazywa się *zarządzania ochroną skoncentrowaną na użytkowniku*. Aby zastosować różne ustawienia aplikacji na różnych urządzeniach, możesz użyć połączonych typów zarządzania. Aby zaimplementować zarządzanie ochroną skoncentrowaną na urządzeniu, możesz użyć narzędzi dostarczonych w Konsoli administracyjnej opartej na Microsoft Management Console lub Kaspersky Security Center Web Console. Zarządzanie ochroną skoncentrowaną na użytkowniku może zostać zaimplementowane tylko poprzez Kaspersky Security Center Web Console.

Zarządzanie bezpieczeństwem skoncentrowane na urządzeniu umożliwia zastosowanie różnych ustawień bezpieczeństwa aplikacji na zarządzanych urządzeniach w zależności od funkcji charakterystycznych dla urządzeń. Na przykład, możesz zastosować różne ustawienia do urządzeń przydzielonych w różnych grupach administracyjnych. Możesz także rozróżnić urządzenia przy użyciu tych urządzeń w Active Directory lub ich specyfikacji sprzętowej.

Zarządzanie bezpieczeństwem skoncentrowanym na użytkowniku umożliwia zastosowanie różnych ustawień aplikacji zabezpieczającej do różnych ról użytkownika. Możesz utworzyć kilka ról użytkownika, przypisać odpowiednią rolę użytkownika do każdego użytkownika oraz określić różne ustawienia aplikacji do urządzeń należących do użytkowników z różnymi rolami. Na przykład, chcesz zastosować różne ustawienia aplikacji na urządzeniach księgowych i specjalistów z działu HR. W rezultacie, gdy zaimplementowane jest zarządzanie ochroną skoncentrowaną na użytkowniku, każdy dział—dział księgowych i dział HR—posiada swoją własną konfigurację ustawień dla aplikacji firmy Kaspersky. Konfiguracja ustawień definiuje, które ustawienia aplikacji mogą być zmieniane przez użytkowników i dla których wymuszone jest ustawienie i zablokowanie przez administratora.

Korzystając z zarządzania ochroną skoncentrowaną na użytkowniku, możesz zastosować określone ustawienia aplikacji do pojedynczych użytkowników. Może to być wymagane, gdy pracownik posiada unikatową rolę w firmie lub gdy chcesz monitorować incydenty bezpieczeństwa dotyczące urządzeń określonej osoby. W zależności od roli tego pracownika w firmie, możesz rozszerzyć lub ograniczyć uprawnienia tej osoby do zmiany ustawień aplikacji. Na przykład, możesz rozszerzyć uprawnienia administratora systemu, który zarządza urządzeniami klienckimi w biurze lokalnym.

Możesz połączyć metody zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku. Na przykład, możesz skonfigurować określony profil aplikacji dla każdej grupy administracyjnej, a następnie utworzyć profile zasad dla jednej lub kilku ról użytkownika Twojej firmy. W tym przypadku profile i profile zasad są stosowane w następującej kolejności:

1. Zostaną zastosowane profile utworzone dla zarządzania ochroną skoncentrowaną na urządzeniu.
2. Są one modyfikowane przez profile zasad zgodnie z priorytetami profili zasad.
3. Profile są modyfikowane przez profile zasad skojarzone z rolami użytkownika.

Ręczna konfiguracja profilu Kaspersky Endpoint Security

W tej sekcji można znaleźć zalecenia dotyczące konfiguracji zasady Kaspersky Endpoint Security, który jest tworzony przez Kreator wstępnej konfiguracji. Możesz przeprowadzić konfigurację w oknie właściwości zasady.

Podczas modyfikowania ustawień należy pamiętać o kliknięciu ikony blokady nad odpowiednim ustawieniem, aby umożliwić jego użycie na stacji roboczej.

Konfigurowanie zasady w sekcji Zaawansowana ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Zaawansowana ochrona przed zagrożeniami** możesz skonfigurować używanie Kaspersky Security Network dla Kaspersky Endpoint Security for Windows. Możesz także skonfigurować moduły Kaspersky Endpoint Security for Windows, takie jak Wykrywanie zachowań, Ochrona przed exploitami, Ochrona przed włamaniami oraz Silnik korygujący.

W podsekcji **Kaspersky Security Network** zalecane jest włączenie opcji **Użyj KSN Proxy**. Użyj tej opcji do redystrybucji i optymalizacji ruchu w sieci. Jeśli opcja **Użyj serwera proxy KSN** jest wyłączona, możesz włączyć bezpośrednie korzystanie z serwerów KSN.

Konfigurowanie profilu w sekcji Podstawowa ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Ochrona przed podstawowymi zagrożeniami** okna właściwości zasad, zalecamy określenie dodatkowych ustawień w podsekcjach **Zapora sieciowa** i **Ochrona plików**.

Podsekcja **Zapora sieciowa** zawiera ustawienia, które pozwalają kontrolować aktywność sieciową aplikacji na urządzeniach klienckich. Urządzenie klienckie korzysta z sieci, do której przypisany jest jeden z następujących statusów: publiczny, lokalny lub zaufany. W zależności od stanu sieci, Kaspersky Endpoint Security może zezwolić na aktywność sieciową na urządzeniu lub jej zabronić. Gdy dodajesz nową sieć do swojej organizacji, musisz przypisać jej odpowiedni status sieci. Na przykład, jeśli urządzeniem klienckim jest laptop, zalecamy, aby to urządzenie korzystało z sieci publicznej lub zaufanej, ponieważ laptop nie zawsze jest podłączony do sieci lokalnej. W podsekcji **Zapora ogniowa** możesz sprawdzić, czy prawidłowo przypisano stany do sieci używanych w Twojej organizacji.

W celu sprawdzenia listy sieci:

1. We właściwościach zasady przejdź do **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa.**
2. W sekcji **Dostępne sieci** kliknij przycisk **Ustawienia**.
3. W **oknie**, które zostanie otwarte, przejdź do zakładki **Sieci**, aby wyświetlić listę sieci.

W podsekcji **Ochrona plików** możesz wyłączyć skanowanie dysków sieciowych. Skanowanie dysków sieciowych może spowodować znaczne obciążenie dysków sieciowych. Praktyczniejsze jest wykonywanie bezpośredniego skanowania na serwerach plików.

W celu wyłączenia skanowania dysków sieciowych:

1. We właściwościach zasady przejdź do **Podstawowej ochrony przed zagrożeniami → Ochrona plików przed zagrożeniami**.
2. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
3. W otwartym oknie **Ochrona plików**, na zakładce **Ogólne** odznacz pole **Wszystkie dyski sieciowe**.

Konfigurowanie profilu w sekcji Ustawienia ogólne

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Ustawienia ogólne** okna właściwości profilu zalecamy określenie dodatkowych ustawień w podsekcjach **Raporty i Przechowywanie** oraz **Interfejs**.

W podsekcji **Raporty i przechowywanie** przejdź do sekcji **Przesyłanie danych na Serwer administracyjny**. Pole **informacji o uruchomionej aplikacji** określa, czy baza danych Serwera administracyjnego zapisuje informacje o wszystkich wersjach wszystkich modułów oprogramowania na urządzeniach sieciowych. Jeśli to pole jest zaznaczone, zapisane informacje mogą wymagać znaczącej ilości miejsca na dysku dla bazy danych Kaspersky Security Center (kilkadziesiąt gigabajtów). Odznacz pole **Informacje o uruchomionych aplikacjach**, jeśli wciąż jest zaznaczone w profilu najwyższego poziomu.

Jeśli Konsola administracyjna zarządza ochroną antywirusową w sieci organizacji w trybie scentralizowanym, wyłącz wyświetlanie interfejsu użytkownika Kaspersky Endpoint Security for Windows na stacjach roboczych. W tym celu w podsekcji **Interfejs** przejdź do sekcji **Interakcja z użytkownikiem**, a następnie wybierz opcję **Nie wyświetlaj**.

Aby włączyć ochronę hasłem na stacjach roboczych, w podsekcji **Interfejs** przejdź do sekcji **Ochrona hasłem**, kliknij przycisk **Ustawienia**, a następnie zaznacz pole **Włącz ochronę hasłem**.

Konfigurowanie profilu w sekcji Konfiguracja zdarzenia

W sekcji **Konfiguracja zdarzenia** należy wyłączyć zapisywanie wszelkich zdarzeń na Serwerze administracyjnym, za wyjątkiem następujących zdarzeń:

- Na zakładce **Zdarzenie krytyczne**:
  - Automatyczne uruchamianie aplikacji jest wyłączone
  - Dostęp zabroniony
  - Zablokowano uruchomienie aplikacji
  - Leczenie nie jest możliwe
  - Umowa licencyjna naruszona
  - Nie można załadować modułu szyfrującego
  - Nie można uruchomić dwóch zadań jednocześnie
  - Wykryto aktywne zagrożenie Uruchom Zaawansowane leczenie
  - Wykryto atak sieciowy
  - Nie wszystkie komponenty zostały zaktualizowane
  - Błąd aktywacji

- Błąd włączenia trybu przenośnego
- Błąd interakcji z Kaspersky Security Center
- Błąd wyłączenia trybu przenośnego
- Błąd zmiany komponentów aplikacji
- Błąd zastosowania reguł szyfrowania/deszyfrowania pliku
- Nie można zastosować profilu
- Proces został przerwany
- Zablokowano aktywność sieciową

- Na karcie **Błąd funkcjonalny**: Nieprawidłowe ustawienia zadania. Ustawienia nie zostały zastosowane
- Na zakładce **Ostrzeżenie**:
  - Autoochrona jest wyłączona
  - Nieprawidłowy klucz zapasowy
  - Użytkownik zrezygnował z profilu szyfrowania
- Na karcie **Informacje**: Uruchamianie aplikacji zabronione w trybie testowym

Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security

Optymalną i zalecaną opcją terminarza dla Kaspersky Endpoint Security w wersji 10 i nowszej jest **Po pobraniu nowych uaktualnień do repozytorium**, gdy zaznaczone jest pole **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security

Kreator wstępnej konfiguracji tworzy grupowe zadanie skanowania urządzeń. Domyślnie skonfigurowano terminarz **uruchamiania zadania w piątki o godzinie 19:00** z automatyczną randomizacją i odznaczonym polem **Uruchom pominięte zadania**.

Oznacza to, że jeśli urządzenia w organizacji są wyłączone w piątki, na przykład o godzinie 18:30, zadanie skanowania urządzeń nigdy nie zostanie uruchomione. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego zadanie *Wyszukiwanie luk i wymaganych aktualizacji.* Domyślnie skonfigurowano terminarz **uruchamiania zadania we wtorki o godzinie 19:00** z automatyczną randomizacją i zaznaczonym polem **Uruchom pominięte zadania**.

Jeśli zasady obowiązujące w organizacji nakazują wyłączenie wszystkich urządzeń w tym czasie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie uruchomione, gdy urządzenia znowu zostaną włączone, czyli w środę rano. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemów dysku. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Ręczna konfiguracja grupowego zadania instalacji uaktualnień i naprawy luk

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego grupowe zadanie instalacji uaktualnień i naprawy luk. Domyślnie skonfigurowano terminarz uruchamiania zadania codziennie o godzinie 01:00 z automatyczną randomizacją i wyłączoną opcją **Uruchom pominięte zadania**.

Jeśli reguły obowiązujące w organizacji nakazują wyłączanie urządzeń na noc, zadanie instalacji uaktualnień nigdy nie zostanie uruchomione. Terminarz dla zadania wykrywania luk należy skonfigurować w oparciu o zasady obowiązujące w organizacji. Należy pamiętać, że zadanie instalacji uaktualnień może wymagać ponownego uruchomienia urządzenia.

Określanie maksymalnej liczby zdarzeń w repozytorium zdarzeń

W sekcji **Repozytorium zdarzeń** okna właściwości Serwera administracyjnego możesz zmodyfikować ustawienia przechowywania zdarzeń w bazie danych Serwera administracyjnego, ograniczając liczbę wpisów zdarzeń i czas przechowywania wpisów. Jeśli określisz maksymalną liczbę zdarzeń, aplikacja oblicza przybliżoną ilość miejsca przechowywania, wymaganą dla określonej liczby. Możesz użyć tego przybliżonego obliczenia do oszacowania wystarczającej ilości wolnego miejsca na dysku, aby uniknąć przepełnienia bazy danych. Domyślna pojemność bazy danych Serwera administracyjnego wynosi 400 000 zdarzeń. Maksymalną dozwoloną pojemnością bazy danych jest 45 milionów zdarzeń.

Jeśli liczba zdarzeń w bazie danych osiągnie maksymalną wartość określoną przez administratora, aplikacja usunie najstarsze zdarzenia i zastąpi je nowymi. Jeśli Serwer administracyjny usuwa starsze zdarzenia, nie może zapisywać nowych zdarzeń do bazy danych. W tym czasie informacje o odrzuconych zdarzeniach są zapisywane w dzienniku zdarzeń aplikacji Kaspersky. Nowe zdarzenia zostają zakolejkowane, a następnie zapisane do bazy danych po zakończeniu operacji usuwania.

Aby ograniczyć liczbę zdarzeń, które mogą być przechowywane w repozytorium zdarzeń na Serwerze administracyjnym:

1. Kliknij Serwer administracyjny prawym klawiszem myszy, a następnie wybierz **Właściwości**.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. W obszarze roboczym sekcji **Repozytorium zdarzeń** określ maksymalną liczbę zdarzeń przechowywanych w bazie danych.

3. Kliknij **OK**.

Dodatkowo możesz zmienić ustawienia dowolnego zadania, aby zapisywać zdarzenia związane z postępem zadania lub zapisywać tylko wyniki wykonania zadania. Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Określenie maksymalnego okresu przechowywania informacji o wyeliminowanych lukach

W celu ustawienia maksymalnego okresu przechowywania w bazie danych informacji o lukach, które zostały już wyeliminowane na zarządzanych urządzeniach:

1. Kliknij Serwer administracyjny prawym klawiszem myszy, a następnie wybierz **Właściwości**.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. W obszarze roboczym sekcji **Repozytorium zdarzeń** określ maksymalny okres przechowywania informacji o wyeliminowanych lukach w bazie danych.

   Domyślnie okres przechowywania wynosi 90 dni.

3. Kliknij **OK**.

Maksymalny okres przechowywania informacji o wyeliminowanych lukach jest ograniczony do określonej liczby dni. Następnie zadanie konserwacji Serwera administracyjnego usunie nieaktualne informacje z bazy danych.

Zarządzanie zadaniami

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

Zadania są podzielone na następujące typy:

- *Zadania grupowe*. Zadania wykonywane na urządzeniach wybranej grupy administracyjnej.
- *Zadania Serwera administracyjnego*. Zadania wykonywane przez Serwer administracyjny.
- *Zadania dla wskazanych urządzeń*. Zadania wykonywane na wybranych urządzeniach, niezależnie od tego, czy znajdują się w jakichkolwiek grupach administracyjnych.
- *Zadania lokalne*. Zadania wykonywane na określonym urządzeniu.

Zadanie aplikacji może być utworzone tylko wtedy, gdy wtyczka zarządzająca tą aplikacją jest zainstalowana na stacji roboczej administratora.

Możesz utworzyć listę urządzeń, dla których zostanie utworzone zadanie, korzystając z jednej z następujących metod:

- Wybierz urządzenia z sieci wykryte przez Serwer administracyjny.

- Ręcznie określ listę urządzeń. Jako adresu urządzenia możesz użyć adresu IP (lub zakresu adresów IP), nazwy NetBIOS lub nazwy DNS.

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

  Jeśli lista urządzeń jest importowana z pliku lub jest tworzona ręcznie, a urządzenia są identyfikowane po nazwie, lista może zawierać tylko urządzenia, o których informacje zostały już dodane do bazy danych Serwera administracyjnego podczas podłączania tych urządzeń lub podczas wyszukiwania urządzeń.

Dla każdej aplikacji można utworzyć dowolną liczbę zadań grupowych, zadań dla wskazanych urządzeń oraz zadań lokalnych.

Wymiana informacji o zadaniach między aplikacją zainstalowaną na urządzeniu a bazą danych Kaspersky Security Center odbywa się podczas łączenia Agenta sieciowego z Serwerem administracyjnym.

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

Zadania są uruchamiane na urządzeniu tylko wtedy, gdy uruchomiona jest aplikacja, dla której utworzono zadanie. Jeżeli aplikacja jest wyłączona, wszystkie uruchomione zadania są anulowane.

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

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

Szczegóły dotyczące zarządzania zadaniami dla aplikacji z obsługą wielodostępności

Zadanie grupowe dla aplikacji z obsługą wielodostępności jest stosowane do aplikacji w zależności od hierarchii Serwerów administracyjnych i urządzeń klienckich. Wirtualny Serwer administracyjny, z którego tworzone jest zadanie, musi znajdować się w tej samej grupie administracyjnej lub w grupie administracyjnej niższego poziomu niż urządzenie klienckie, na którym zainstalowana jest aplikacja.

W zdarzeniach, które odpowiadają wynikom wykonania zadania, administratorowi dostawcy usługi wyświetlane są informacje o urządzeniu, na którym wykonywane jest zadanie. Natomiast administratorowi dzierżawczemu wyświetlany jest **Węzeł wielodostępowy**.

Tworzenie zadania

W Konsoli administracyjnej możesz tworzyć zadania bezpośrednio w folderze grupy administracyjnej, dla której tworzone jest zadanie grupowe, lub w obszarze roboczym folderu **Zadania**.

W celu utworzenia zadania grupowego w folderze grupy administracyjnej:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz utworzyć zadanie.

2. W obszarze roboczym grupy wybierz zakładkę **Zadania**.

3. Uruchom tworzenie zadania, klikając przycisk **Utwórz zadanie**.

Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

*W celu utworzenia zadania w obszarze roboczym folderu **Zadania**:*

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania, klikając przycisk **Zakończ**.

Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

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

Tworzenie zadania Serwera administracyjnego

Serwer administracyjny wykonuje następujące zadania:

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

Na wirtualnym Serwerze administracyjnym dostępne jest tylko zadanie automatycznego dostarczania raportów oraz zadanie tworzenia pakietu instalacyjnego z obrazu systemu operacyjnego odpowiedniego urządzenia. Repozytorium wirtualnego Serwera administracyjnego wyświetla uaktualnienia pobrane na główny Serwer administracyjny. Kopia zapasowa danych wirtualnego Serwera administracyjnego jest wykonywana wraz z kopią zapasową danych głównego Serwera administracyjnego.

W celu utworzenia zadania Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - W drzewie konsoli, z menu kontekstowego folderu **Zadania** wybierz **Nowe** → **Zadanie**.
   - Kliknij przycisk **Utwórz zadanie** dostępny w obszarze roboczym folderu **Zadania**.

Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

Zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego, Wykonaj synchronizację Windows Update, Konserwacja baz danych i *Utwórz kopię zapasową danych Serwera administracyjnego* mogą zostać utworzone tylko raz. Jeśli zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*, *Konserwacja baz danych*, *Kopia zapasowa danych Serwera administracyjnego* i *Wykonaj synchronizację Windows Update* zostały już utworzone dla Serwera administracyjnego, nie będą wyświetlane w oknie wyboru typu zadania Kreatora nowych zadań.

Tworzenie zadania dla określonych urządzeń

W Kaspersky Security Center możliwe jest utworzenie zadań dla określonych urządzeń. Urządzenia połączone w zbiór mogą należeć do różnych grup administracyjnych lub nie należeć do żadnej grupy administracyjnej. Kaspersky Security Center może wykonać następujące główne zadania dla określonych urządzeń:

- Zdalnie zainstalować aplikację
- Wysłać wiadomość do użytkownika
- Zmienić Serwer administracyjny
- Zarządzać urządzeniami
- Zweryfikować uaktualnienia
- Rozesłać pakiety instalacyjne
- Zdalnie zainstaluj aplikację na podrzędnych Serwerach administracyjnych
- Zdalnie odinstalować aplikację

W celu utworzenia zadania dla określonych urządzeń:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - Wybierając **Nowe** → **Zadanie** w menu kontekstowym folderu **Zadania** w drzewie konsoli.
   - Kliknij przycisk **Utwórz zadanie** dostępny w obszarze roboczym folderu **Zadania**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

Tworzenie zadania lokalnego

W celu utworzenia zadania lokalnego dla urządzenia:

1. W obszarze roboczym grupy zawierającej urządzenie wybierz zakładkę **Urządzenia**.
2. Z listy urządzeń na zakładce **Urządzenia** wybierz urządzenie, dla którego powinno zostać utworzone zadanie lokalne.

3. Uruchom tworzenie zadania dla wybranego urządzenia w jeden z następujących sposobów:

   - Kliknij przycisk **Wykonaj akcję** i z listy rozwijalnej wybierz wartość **Utwórz zadanie**.
   - Kliknij przycisk **Utwórz zadanie** w obszarze roboczym urządzenia.
   - Zastosuj właściwości urządzenia w następujący sposób:

     a. Z otwartego menu kontekstowego urządzenia wybierz **Właściwości**.

     b. W oknie właściwości urządzenia, które zostanie otwarte, przejdź do sekcji **Zadania** i kliknij **Dodaj**.

Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

Szczegółowe instrukcje dotyczące sposobu tworzenia i konfiguracji zadań lokalnych są dostępne w podręcznikach dla odpowiednich aplikacji firmy Kaspersky.

Wyświetlanie dziedziczonego zadania grupowego w obszarze roboczym grupy zagnieżdżonej

W celu włączenia wyświetlania dziedziczonych zadań grupy zagnieżdżonej w obszarze roboczym:

1. W obszarze roboczym grupy zagnieżdżonej wybierz zakładkę **Zadania**.
2. W obszarze roboczym zakładki **Zadania** kliknij przycisk **Pokaż zadania dziedziczone**.

Zadania dziedziczone zostaną wyświetlone na liście zadań z jedną z poniższych ikon:

-  — jeśli były dziedziczone od grupy utworzonej na głównym Serwerze administracyjnym.
-  — jeśli były dziedziczone od grupy z wyższego poziomu hierarchii.

Jeżeli włączony jest tryb dziedziczenia, zadania dziedziczone będą mogły być modyfikowane tylko w grupie, w której zostały utworzone. Zadania dziedziczone nie mogą być modyfikowane w grupie, która dziedziczy zadania.

Automatyczne włączanie urządzeń przed uruchomieniem zadania

Kaspersky Security Center nie uruchamia zadań na wyłączonych urządzeniach. Możesz skonfigurować Kaspersky Security Center, aby automatycznie włączał te urządzenia przed uruchomieniem zadania, korzystając z funkcji Wake-on-LAN.

W celu skonfigurowania automatycznego uruchamiania urządzeń przed uruchomieniem zadania:

1. W oknie ustawień zadania wybierz sekcję **Terminarz**.
2. Aby skonfigurować działania na urządzeniach, kliknij łącze **Zaawansowane**.
3. W otwartym oknie **Zaawansowane** zaznacz pole **Włącz urządzenia przed uruchomieniem zadania (min) przy użyciu funkcji Wake-on-LAN** i określ przedział czasu w minutach.

W rezultacie na określoną liczbę minut przed uruchomieniem zadania Kaspersky Security Center włącza urządzenia i ładuje na nich system operacyjny za pomocą funkcji Wake-on-LAN. Po zakończeniu zadania urządzenia są automatycznie wyłączane, jeśli użytkownicy urządzeń nie zalogują się do systemu. Zauważ, że Kaspersky Security Center automatycznie wyłącza tylko te urządzenia, które są włączone przy użyciu funkcji Wake-on-LAN.

Kaspersky Security Center może automatycznie uruchamiać systemy operacyjne tylko na urządzeniach obsługujących standard Wake-on-LAN (WoL).

Automatyczne wyłączanie urządzenia po zakończeniu zadania

Kaspersky Security Center umożliwia konfigurowanie zadania w taki sposób, że urządzenia, do których się odnoszą, są automatycznie wyłączane po zakończeniu zadania.

W celu automatycznego wyłączenia urządzenia po zakończeniu zadania:

1. W oknie ustawień zadania wybierz sekcję **Terminarz**.
2. Kliknij odnośnik **Zaawansowane**, aby otworzyć okno, w którym można skonfigurować działania na urządzeniach.
3. W otwartym oknie **Zaawansowane** zaznacz pole **Wyłącz urządzenia po zakończeniu zadania**.

Ograniczanie czasu uruchamiania zadania

W celu ograniczenia czasu, w trakcie którego zadanie jest uruchamiane na urządzeniach:

1. W oknie ustawień zadania wybierz sekcję **Terminarz**.
2. Otwórz okno konfiguracji akcji wykonywanych na urządzeniach klienckich, klikając **Zaawansowane**.
3. W otwartym oknie **Zaawansowane** zaznacz pole **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż (min)** i określ przedział czasu w minutach.

   Jeżeli zadanie na urządzeniu nie zostało jeszcze zakończone po minięciu określonego przedziału czasu, Kaspersky Security Center automatycznie zatrzyma wykonywanie zadania.

Eksportowanie zadania

Zadania grupowe oraz zadania dla wskazanych urządzeń można wyeksportować do pliku. Nie można eksportować zadań Serwera administracyjnego i zadań lokalnych.

W celu wyeksportowania zadania:

1. Z otwartego menu kontekstowego zadania wybierz **Wszystkie zadania → Eksportuj**.
2. W otwartym oknie **Zapisz jako** określ ścieżkę pliku.

3. Kliknij przycisk **Zapisz**.

Uprawnienia użytkowników lokalnych nie są eksportowane.

Importowanie zadania

Możliwe jest zaimportowanie zadań grupowych oraz zadań dla wskazanych urządzeń. Nie można importować zadań Serwera administracyjnego i zadań lokalnych.

W celu zaimportowania zadania:

1. Wybierz listę, do której ma zostać zaimportowane zadanie:
   - Jeżeli chcesz zaimportować zadanie do listy zadań grupowych, w obszarze roboczym żądanej grupy administracyjnej wybierz zakładkę **Zadania**.
   - Jeżeli chcesz zaimportować zadanie do listy zadań dla wskazanych urządzeń, w drzewie konsoli wybierz folder **Zadania**.
2. W celu zaimportowania zadania wybierz jedną z następujących opcji:
   - Z menu kontekstowego listy zadań wybierz **Wszystkie zadania → Importuj**.
   - Kliknij odnośnik **Importuj zadanie z pliku** w sekcji zarządzania listą zadań.
3. W otwartym oknie określ ścieżkę dostępu do pliku, z którego chcesz zaimportować zadanie.
4. Kliknij przycisk **Otwórz**.

   Zadanie będzie wyświetlane na liście zadań.

Jeśli nowo importowane zadanie ma identyczną nazwę jak istniejące zadanie, nazwa importowanego zadania jest rozszerzana o indeks **(<następny numer porządkowy>)**, na przykład: **(1)**, **(2)**.

Konwertowanie zadań

Przy pomocy Kaspersky Security Center możesz konwertować zadania z poprzednich wersji aplikacji Kaspersky do zadań z aktualnych wersji tych aplikacji.

Konwersja jest dostępna dla zadań następujących aplikacji:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

W celu konwertowania zadań:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz skonwertować zadania.
2. W menu kontekstowym Serwera administracyjnego wybierz **Wszystkie zadania → Kreator konwersji zasad i zadań**.

Zostanie uruchomiony Kreator konwersji zasad i zadań. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu pracy kreatora zostaną utworzone nowe zadania, które korzystają z ustawień zadań z poprzednich wersji aplikacji.

Ręczne uruchamianie i zatrzymywanie zadania

Zadania można uruchamiać i zatrzymywać ręcznie przy użyciu jednej z następujących metod: z poziomu menu kontekstowego zadania lub w oknie właściwości urządzenia klienckiego, do którego zadanie zostało przypisane.

Uruchamianie zadań grupowych z poziomu menu kontekstowego urządzenia jest dozwolone tylko dla użytkowników należących do grupy **KLAdmins**.

W celu uruchomienia lub zatrzymania zadania z poziomu menu kontekstowego lub okna właściwości zadania:

1. Z listy zadań wybierz zadanie.
2. Uruchom lub zatrzymaj zadanie w jeden z następujących sposobów:
   - Wybierając **Uruchom** lub **Zatrzymaj** w menu kontekstowym zadania.
   - Klikając **Uruchom** lub **Zatrzymaj** w sekcji **Ogólny** okna właściwości zadania.

W celu uruchomienia lub zatrzymania zadania z poziomu menu kontekstowego lub okna właściwości urządzenia klienckiego:

1. Z listy urządzeń wybierz urządzenie.
2. Uruchom lub zatrzymaj zadanie w jeden z następujących sposobów:
   - Wybierając **Wszystkie zadania → Uruchom zadanie** z menu kontekstowego urządzenia. Wybierz odpowiednie zadanie z listy zadań.

     Lista urządzeń, do których zadanie jest przypisane, zostanie zastąpiona wybranym urządzeniem. Zadanie zostanie uruchomione.
   - Klikając przycisk () lub () w sekcji **Zadania** okna właściwości urządzenia.

Ręczne wstrzymywanie i wznawianie zadania

W celu ręcznego wstrzymania lub wznowienia wykonywania zadania:

1. Z listy zadań wybierz zadanie.
2. Wstrzymaj lub wznów zadanie w jeden z następujących sposobów:
   - Wybierając **Wstrzymaj** lub **Wznów** w menu kontekstowym zadania.
   - Wybierając sekcję **Ogólny** w oknie właściwości i klikając **Wstrzymaj** lub **Wznów**.

Monitorowanie wykonywania zadania

W celu monitorowania wykonywania zadania:

W oknie ustawień zadania wybierz sekcję **Ogólny**.

W środkowej części sekcji **Ogólny** wyświetlany jest bieżący stan zadania.

Przeglądanie wyników wykonywania zadań przechowywanych na Serwerze administracyjnym

Kaspersky Security Center umożliwia przeglądanie wyników wykonywania zadań grupowych, zadań dla wskazanych urządzeń oraz zadań Serwera administracyjnego. Nie można przeglądać wyników wykonywania zadań lokalnych.

W celu przejrzenia wyników wykonania zadania:

1. W oknie właściwości zadania wybierz sekcję **Ogólny**.
2. Kliknij odnośnik **Wyniki**, aby otworzyć okno **Wyniki zadania**.

Konfigurowanie filtrowania informacji o wynikach wykonywania zadań

Kaspersky Security Center umożliwia filtrowanie informacji o wynikach wykonywania zadań grupowych, zadań dla wskazanych urządzeń oraz zadań Serwera administracyjnego. Opcja filtrowania nie jest dostępna dla zadań lokalnych.

W celu skonfigurowania filtrowania informacji o wynikach wykonywania zadania:

1. W oknie właściwości zadania wybierz sekcję **Ogólny**.
2. Kliknij odnośnik **Wyniki**, aby otworzyć okno **Wyniki zadania**.

   Tabela w górnej części okna zawiera listę wszystkich urządzeń, do których przydzielono zadanie. Tabela w dolnej części okna wyświetla wyniki zadania wykonywanego na wybranym urządzeniu.
3. Kliknij prawym klawiszem myszy odpowiednią tabelę, aby otworzyć menu kontekstowe, z którego wybierz **Filtr**.
4. W otwartym oknie **Ustaw filtr** zdefiniuj ustawienia filtra w sekcjach: **Zdarzenia**, **Urządzenia** i **Czas**. Kliknij **OK**.

Okno **Wyniki zadania** będzie wyświetlało informacje odpowiadające ustawieniom określonym w filtrze.

Modyfikowanie zadania. Wycofywanie zmian

W celu zmodyfikowania zadania:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W obszarze roboczym folderu **Zadania** wybierz zadanie i przejdź do okna właściwości zadania, korzystając z menu kontekstowego.
3. Wprowadź niezbędne zmiany.

   W sekcji **Wykluczenia z zakresu zadania** możesz skonfigurować listę podgrup, do których zadanie nie jest stosowane.

4. Kliknij **Zastosuj**.

Zmiany wprowadzone w zadaniu zostaną zapisane w oknie właściwości zadania, w sekcji **Historia rewizji**.

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w zadaniu.

W celu wycofania zmian wprowadzonych w zadaniu:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Wybierz zadanie, w którym należy wycofać zmiany, i przejdź do okna właściwości zadania, korzystając z menu kontekstowego.
3. W oknie właściwości zadania wybierz sekcję **Historia rewizji**.
4. Na liście rewizji zadania wybierz numer rewizji, do której chcesz wycofać zmiany.
5. Kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz wartość **Wycofaj**.

Porównywanie zadań

Możesz porównać zadania tego samego typu: na przykład, możesz porównać dwa zadania skanowania w poszukiwaniu złośliwego oprogramowania, ale nie możesz porównać zadania skanowania pod kątem złośliwego oprogramowania i zadania instalacji aktualizacji. Po zakończeniu porównywania, uzyskasz raport wyszczególniający te ustawienia, które są takie same, oraz te, które są różne. Raport z porównania zadań można wydrukować lub zapisać do pliku. Porównanie zadań może być przydatne, gdy różne jednostki w firmie posiadają przypisane różne zadania tego samego typu. Na przykład, na komputerach pracowników z działu księgowości jest ustawione zadanie skanowania w poszukiwaniu złośliwego oprogramowania tylko dysków lokalnych, a na komputerach pracowników z działu sprzedaży ustawione jest zadanie skanowania antywirusowego dysków lokalnych i poczty. Nie musisz przeglądać wszystkich ustawień zadania, aby zauważyć tę różnicę. Wystarczy szybkie porównanie zadań.

Porównywać można tylko zadania tego samego typu.

Porównanie może odbywać się tylko parami.

Zadania można porównać w jeden z następujących sposobów: poprzez wybranie jednego zadania i porównanie go z innym lub poprzez porównanie dowolnych dwóch zadań z listy zadań.

W celu wybrania jednego zadania i porównanie go z innym:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W obszarze roboczym folderu **Zadania** wybierz zadanie, które chcesz porównać z innym.
3. Z otwartego menu kontekstowego zadania wybierz **Wszystkie zadania** → **Porównaj z innym zadaniem**.
4. W oknie **Wybierz zadanie** wybierz zadanie do porównania.
5. Kliknij **OK**.

   Zostanie wyświetlony raport w formacie HTML z porównaniem dwóch zadań.

W celu porównania dwóch dowolnych zadań z listy zadań:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. W folderze **Zadania**, na liście zadań wciśnij klawisz **`Shift`** lub **`Ctrl`**, aby wybrać dwa zadania tego samego typu.
3. Z menu kontekstowego wybierz **Porównaj**.

   Zostanie wyświetlony raport w formacie HTML z porównaniem wybranych zadań.

Podczas porównywania zadań, gdy hasła różnią się, w raporcie z porównania zadań wyświetlane są gwiazdki (******).

Jeśli hasło zostało zmienione we właściwościach zadania, gwiazdki (******) są wyświetlane w raporcie z porównania rewizji (******).

Konta do uruchamiania zadań

Możesz określić konto, z poziomu którego ma być uruchamiane zadanie.

Na przykład, aby uruchomić zadanie skanowania na żądanie, musisz posiadać uprawnienia dostępu do skanowanego obiektu, natomiast żeby uruchomić zadanie aktualizacji, musisz posiadać uprawnienia autoryzowanego użytkownika serwera proxy. Możliwość określenia konta dla uruchamiania zadania pozwala uniknąć problemów z zadaniami skanowania na żądanie i zadaniami aktualizacji w sytuacji, gdy użytkownik uruchamiający zadanie nie posiada żądanych uprawnień dostępu.

Podczas wykonywania zadań zdalnej instalacji / dezinstalacji określone konto jest używane do pobierania na urządzenia klienckie plików wymaganych do zainstalowania / odinstalowania aplikacji w przypadku, gdy Agent sieciowy nie jest zainstalowany lub jest niedostępny. Jeśli Agent sieciowy jest zainstalowany i jest dostępny, konto jest używane, gdy zgodnie z ustawieniami zadań, dostarczanie plików jest wykonywane tylko przy użyciu narzędzi systemu Microsoft Windows z folderu współdzielonego. W tej sytuacji konto musi posiadać na urządzeniu następujące uprawnienia:

- Uprawnienie do zdalnego uruchamiania aplikacji.
- Uprawnienie do używania zasobu Admin$.
- Uprawnienie do *Zalogowania w trybie usługi*.

Jeśli pliki są dostarczane na urządzenia przez Agenta sieciowego, konto nie będzie używane. Wówczas wszystkie działania kopiowania i instalacji są wykonywane przez **Agenta sieciowego** (**konto LocalSystem**).

Kreator zmiany haseł w zadaniach

Dla zadania, które nie jest lokalne, możesz określić konto, z poziomu którego zadanie musi być uruchomione. Konto może zostać określone podczas tworzenia zadania lub we właściwościach istniejącego zadania. Jeśli określone konto jest używane zgodnie z instrukcjami bezpieczeństwa organizacji, te instrukcje mogą wymagać zmiany hasła do konta od czasu do czasu. Jeśli hasło do konta wygaśnie i ustawisz nowe, nie powiedzie się uruchomienie zadań, aż do momentu, gdy określisz nowe ważne hasło we właściwościach zadania.

Kreator zmiany haseł w zadaniach umożliwia automatyczne zastąpienie starego hasła nowym we wszystkich zadaniach, w których konto jest określone. Alternatywnie, możesz zrobić to ręcznie we właściwościach każdego zadania.

W celu uruchomienia kreatora zmiany haseł w zadaniach:

1. Z drzewa konsoli wybierz węzeł **Zadania**.
2. Z menu kontekstowego węzła wybierz **Kreator zmiany haseł w zadaniach**.

Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Określanie danych uwierzytelniających

W polach **Konto** i **Hasło** określ nowe dane uwierzytelniające, które aktualnie są ważne w Twoim systemie (na przykład, w Active Directory). Jeśli przejdziesz do następnego kroku kreatora, Kaspersky Security Center sprawdzi, czy nazwa określonego konta odpowiada nazwie konta we właściwościach każdego zadania, które nie jest lokalne. Jeśli nazwy kont pasują do siebie, hasło we właściwościach zadania zostanie automatycznie zastąpione nowym.

Jeśli uzupełnisz pole **Stare hasło (opcjonalnie)**, Kaspersky Security Center zastępuje hasło tylko dla tych zadań, w których zostanie wykryta nazwa konta oraz stare hasło. Zastępowanie odbywa się automatycznie. We wszystkich pozostałych przypadkach musisz wybrać działanie, jakie ma zostać podjęte w kolejnym kroku kreatora.

Krok 2. Wybieranie działania, jakie ma zostać podjęte

Jeśli nie określiłeś starego hasła w pierwszym kroku kreatora lub stare hasło nie odpowiada hasłom w zadaniach, powinieneś wybrać działanie, jakie ma zostać wykonane na wykrytych zadaniach.

Dla każdego zadania, które posiada stan *Wymaga zatwierdzenia*, zdecyduj, czy chcesz usunąć hasło we właściwościach zadania lub zastąpić je nowym. Jeśli zdecydujesz się usunąć hasło, zadanie zostanie przełączone do uruchamiania z poziomu domyślnego konta.

Krok 3. Sprawdzanie wyników

W ostatnim kroku kreatora przejrzyj wyniki dla każdego wykrytego zadania. Aby zakończyć działanie kreatora, kliknij przycisk **Zakończ**.

Tworzenie hierarchii grup administracyjnych podległych wirtualnemu Serwerowi administracyjnemu

Po utworzeniu wirtualnego Serwera administracyjnego zawiera on domyślnie grupę administracyjną o nazwie **Zarządzane urządzenia**.

Procedura tworzenia hierarchii grup administracyjnych podległych wirtualnemu Serwerowi administracyjnemu jest identyczna jak procedura tworzenia hierarchii grup administracyjnych podległych fizycznemu Serwerowi administracyjnemu.

Nie możesz dodawać podrzędnych i wirtualnych Serwerów administracyjnych do grup administracyjnych podległych wirtualnemu Serwerowi administracyjnemu. Dzieje się tak ze względu na ograniczenia wirtualnych Serwerów administracyjnych.

Profile i profile zasad

W Kaspersky Security Center Web Console możesz tworzyć zasady dla aplikacji Kaspersky. Ta sekcja opisuje profile i profile zasad, a także zawiera instrukcje dotyczące ich tworzenia i modyfikowania.

Hierarchia profili i korzystanie z profili

W tej sekcji można znaleźć informacje dotyczące stosowania profili do urządzeń w grupach administracyjnych. Ta sekcja zawiera również informacje o profilach zasad.

Hierarchia profili

W Kaspersky Security Center profile są używane do określenia jednego zestawu ustawień dla kilku urządzeń. Na przykład, obszar profilu aplikacji P zdefiniowanej dla grupy administracyjnej G zawiera zarządzane urządzenia z zainstalowaną aplikacją P, które zostały dodane do grupy G i wszystkich jej podgrup, za wyjątkiem podgrup, we właściwościach których odznaczono opcję **Dziedzicz z grupy nadrzędnej**.

Profil można odróżnić od lokalnego ustawienia po ikonach kłódki (🔒) obok jego ustawień. Jeśli ustawienie (lub grupa ustawień) jest zablokowane we właściwościach zasady, w pierwszej kolejności należy użyć tego ustawienia (lub grupy ustawień) podczas tworzenia obowiązującego ustawienia, a następnie należy zapisać ustawienie (lub grupę ustawień) do zasady podrzędnej.

Tworzenie obowiązujących ustawień można opisać w następujący sposób: wartości wszystkich ustawień, które nie zostały zablokowane, są kopiowane z profilu, a następnie są nadpisywane przez wartości ustawień lokalnych, a w kolejnym etapie wartości wynikowe są nadpisywane przez zablokowane ustawienia pobrane z profilu.

Profile tej samej aplikacji oddziałują na siebie poprzez hierarchię grup administracyjnych: Zablokowane ustawienia z profilu nadrzędnego nadpisują te same ustawienia z profilu podrzędnego.

Dla użytkowników mobilnych istnieje specjalny profil. Ten profil jest aktywowany na urządzeniu, gdy to przełącza się do trybu użytkownika mobilnego. Zasady użytkowników mobilnych nie oddziałują na inne zasady poprzez hierarchię grup administracyjnych.

Profil użytkownika mobilnego nie będzie obsługiwany w kolejnych wersjach Kaspersky Security Center. Zamiast profili użytkowników mobilnych będą używane profile zasad.

Profile zasad

Stosowanie profili na urządzeniach tylko poprzez hierarchię grup administracyjnych może być niewygodne tylko w kilku przypadkach. Konieczne może być utworzenie kilku instancji jednego profilu, które różnią się jednym lub dwoma ustawieniami dla różnych grup administracyjnych, oraz zsynchronizowanie zawartości tych profili w przyszłości.

Aby uniknąć takich problemów, Kaspersky Security Center obsługuje *profile zasad*. Profil zasad jest to inaczej podzbiór ustawień profilu. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z profilem i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od "podstawowego" profilu, który jest aktywny na urządzeniu klienckim (komputerze lub urządzeniu mobilnym). Aktywacja profilu zmodyfikuje ustawienia zasad, które były aktywne na urządzeniu przed aktywacją profilu. Te ustawienia przyjmują wartości określone w profilu.

Aktualnie na profile zasad nałożone są następujące ograniczenia:

- Profil może zawierać maksymalnie 100 profili.
- Profil zasad nie może zawierać innych profili.
- Profil zasad nie może zawierać ustawień powiadamiania.

Zawartość profilu

Profil zasad zawiera następujące elementy:

- Profile z takimi samymi nazwami wpływają na siebie poprzez hierarchię grup administracyjnych ze wspólnymi regułami.
- Podzbiór ustawień profilu. Profil zawiera tylko aktualnie wymagane ustawienia (ustawienia zablokowane).
- Warunek aktywacji to wyrażenie logiczne z właściwościami urządzenia. Profil jest aktywny (uzupełnia zasadę) tylko wtedy, gdy warunek aktywacji profilu jest prawdziwy. We wszystkich pozostałych przypadkach profil jest nieaktywny i jest ignorowany. W wyrażeniu logicznym mogą być uwzględnione następujące właściwości urządzenia:
  - Stan trybu użytkownika mobilnego.
  - Właściwości środowiska sieciowego — nazwa aktywnej reguły dla połączenia z Agentem sieciowym.

- Obecność lub brak określonych znaczników na urządzeniu.
- Lokalizacja urządzenia w jednostce Active Directory: jawna (urządzenie znajduje się w określonej jednostce OU) lub niejawna (urządzenie jest w jednostce OU, która znajduje się w określonej jednostce OU na dowolnym poziomie zagnieżdżenia).
- Członkostwo urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).
- Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).

- Pole wyłączające profil. Wyłączone profile są zawsze ignorowane, a ich odpowiednie warunki aktywacji nie są sprawdzane.
- Priorytet profilu. Warunki aktywacji różnych profili są niezależne, a więc można aktywować kilka profili jednocześnie. Jeśli aktywne profile zawierają nienakładające się na siebie zbiory ustawień, nie pojawi się żaden problem. Jednakże dwa aktywne profile zawierające różne wartości tego samego ustawienia spowodują niejednoznaczność. Tę niejednoznaczność można wyeliminować poprzez priorytety profilu: Wartość niejednoznacznej zmiennej zostanie pobrana z profilu, który ma wyższy priorytet (ten, który znajduje się wyżej na liście profili).

Zachowanie profili, gdy zasady oddziałują na siebie poprzez hierarchię

Profile o tych samych nazwach zostają scalone zgodnie z regułami scalania profilu. Profile zasady nadrzędnej mają wyższy priorytet niż zasady podrzędnej. Jeśli modyfikowanie ustawień jest zabronione w zasadzie nadrzędnej (są zablokowane), zasada podrzędna używa warunków aktywacji profilu z zasady nadrzędnej. Jeśli modyfikowanie ustawień jest dozwolone w zasadzie nadrzędnej, używane są warunki aktywacji profilu z zasady podrzędnej.

Ponieważ w swoim warunku aktywacji profil zasad może zawierać opcję **Urządzenie jest w trybie offline**, profile całkowicie zastępują funkcję profili dla użytkowników mobilnych, które nie będą już obsługiwane.

Profil dla użytkowników mobilnych może zawierać profile, ale te profile mogą zostać aktywowane dopiero po przełączeniu urządzenia w tryb użytkownika mobilnego.

Dziedziczenie ustawień profilu

Profil jest określony dla grupy administracyjnej. Ustawienia profilu mogą być *dziedziczone*, czyli otrzymywane w podgrupach (grupach potomnych) grupy administracyjnej, dla której zostały określone. Dalej profil dla grupy nadrzędnej jest też zwany *zasadą nadrzędną*.

Możesz włączyć lub wyłączyć dwie opcje dziedziczenia: **Dziedzicz ustawienia z zasady nadrzędnej** i **Wymuś dziedziczenie ustawień w zasadach podrzędnych**:

- Jeśli włączysz **Dziedzicz ustawienia z zasady nadrzędnej** dla profilu potomnego i zablokuj niektóre ustawienia w profilu nadrzędnym, wówczas nie będziesz mógł zmienić tych ustawień dla grupy potomnej. Jednakże możesz zmienić ustawienia, które nie są zablokowane w profilu nadrzędnym.
- Jeśli wyłączysz **Dziedzicz ustawienia z zasady nadrzędnej** dla profilu potomnego, wówczas możesz zmienić wszystkie ustawienia w grupie potomnej nawet wtedy, gdy niektóre ustawienia są zablokowane w profilu nadrzędnym.
- Jeśli włączysz **Wymuś dziedziczenie ustawień w zasadach podrzędnych** w grupie nadrzędnej, spowoduje to włączenie **Dziedzicz ustawienia z zasady nadrzędnej** dla każdego profilu potomnego. W tym przypadku nie możesz wyłączyć tej opcji dla żadnego profilu potomnego. Wszystkie ustawienia, które są zablokowane w profilu nadrzędnym, są dziedziczone w grupach potomnych w sposób wymuszony i nie możesz zmienić tych ustawień w grupach potomnych.

- W profilach dla grupy **Zarządzane urządzenia** opcja **Dziedzicz ustawienia z zasady nadrzędnej** nie wpływa na żadne ustawienia, ponieważ grupa **Zarządzane urządzenia** nie zawiera żadnych grup wyższego poziomu i dlatego nie dziedziczy żadnych profili.

Domyślnie, opcja **Wymuś dziedziczenie ustawień w zasadach podrzędnych** jest włączona dla nowego profilu.

Jeśli profil zawiera profile, wszystkie profile potomne dziedziczą te profile.

Zarządzanie profilami

Ustawienia aplikacji zainstalowanych na urządzeniach klienckich są konfigurowane centralnie poprzez definiowanie profili.

Profile utworzone dla aplikacji w grupie administracyjnej są wyświetlane w obszarze roboczym, na zakładce **Zasady**. Przed nazwą każdego profilu wyświetlana jest ikona z jego stanem.

Po usunięciu lub anulowaniu profilu aplikacja będzie kontynuowała działanie z ustawieniami określonymi w profilu. Te ustawienia mogą być później modyfikowane ręcznie.

Stosowanie profilu odbywa się w następujący sposób: jeśli na urządzeniu uruchomione są zadania rezydentne (zadania ochrony w czasie rzeczywistym), ich wykonywanie będzie kontynuowane z użyciem nowych wartości. Każde uruchamiane zadanie okresowe (skanowanie na żądanie, aktualizacja baz danych aplikacji) działa z niezmienionymi wartościami ustawień. Następnym razem zostają uruchomione z nowymi wartościami ustawień.

Profile dla aplikacji z obsługą wielodostępności są dziedziczone przez grupy administracyjne niższego poziomu, a także przez grupy administracyjne wyższego poziomu: profil jest przekazywany do wszystkich urządzeń klienckich, na których zainstalowana jest aplikacja.

W przypadku, gdy Serwery administracyjne są ułożone hierarchicznie, podrzędne Serwery administracyjne otrzymają zasady od głównego Serwera administracyjnego, a następnie rozprowadzą je do urządzeń klienckich. Jeżeli włączone jest dziedziczenie, ustawienia zasady mogą być modyfikowane na głównym Serwerze administracyjnym. Następnie wszelkie zmiany dokonane w ustawieniach zasady są wprowadzane w zasadach dziedziczonych na podrzędnych Serwerach administracyjnych.

Jeżeli połączenie między głównym Serwerem administracyjnym a podrzędnym Serwerem administracyjnym zostanie zerwane, zasada na Serwerze podrzędnym nadal będzie używała zastosowanych ustawień. Ustawienia zasady modyfikowane na głównym Serwerze administracyjnym są rozsyłane do podrzędnego Serwera administracyjnego po ponownym nawiązaniu z nim połączenia.

Jeśli dziedziczenie jest wyłączone, ustawienia zasady mogą być modyfikowane na podrzędnym Serwerze administracyjnym niezależnie od głównego Serwera administracyjnego.

W przypadku, gdy połączenie między Serwerem administracyjnym a urządzeniem klienckim zostanie zerwane, urządzenie klienckie rozpocznie pracę z profilem użytkownika mobilnego (jeśli został określony) lub profil będzie dalej używał zastosowanych ustawień, aż do ponownego nawiązania połączenia.

Wyniki przesłania zasady do podrzędnego Serwera administracyjnego są wyświetlane w oknie właściwości zasady konsoli na głównym Serwerze administracyjnym.

Wyniki przesłania profili do urządzeń klienckich są wyświetlane w oknie właściwości profilu Serwera administracyjnego, z którym są połączone.

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

Tworzenie zasady

W Konsoli administracyjnej możesz tworzyć profile bezpośrednio w folderze grupy administracyjnej, dla której tworzony jest profil, lub w obszarze roboczym folderu **Zasady**.

W celu utworzenia profilu w folderze grupy administracyjnej:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której ma zostać utworzony profil.
2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.
3. Uruchom Kreator tworzenia nowej zasady, klikając przycisk **Nowa zasada**.

   Zostanie uruchomiony Kreator tworzenia nowej zasady. Postępuj zgodnie z instrukcjami kreatora.

*W celu utworzenia profilu w obszarze roboczym folderu **Zasady**:*

1. Z drzewa konsoli wybierz folder **Zasady**.
2. Uruchom Kreator tworzenia nowej zasady, klikając przycisk **Nowa zasada**.

   Zostanie uruchomiony Kreator tworzenia nowej zasady. Postępuj zgodnie z instrukcjami kreatora.

Dla jednej aplikacji z grupy możliwe jest utworzenie kilku profili, ale tylko jeden z nich może być aktywny. Po utworzeniu nowego aktywnego profilu poprzedni staje się nieaktywny.

Podczas tworzenia profilu można skonfigurować minimalny zestaw ustawień wymaganych do prawidłowego działania aplikacji. Wszystkie pozostałe ustawienia posiadają domyślne wartości stosowane podczas lokalnej instalacji aplikacji. Po utworzeniu profilu możesz go zmienić.

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

Ustawienia aplikacji firmy Kaspersky, które zostają zmienione po zastosowaniu profili, zostały szczegółowo opisane w odpowiednich dokumentach.

Po utworzeniu profilu ustawienia, których modyfikowanie zostało zablokowane (ustawiona jest ikona kłódki ( )), będą obowiązywać na urządzeniach klienckich niezależnie od tego, które ustawienia były wcześniej określone dla aplikacji.

Wyświetlanie profilu dziedziczonego w podgrupie

W celu włączenia wyświetlania profili dziedziczonych dla zagnieżdżonej grupy administracyjnej:

1. W drzewie konsoli wybierz grupę administracyjną, dla której powinny być wyświetlane profile dziedziczone.
2. W obszarze roboczym wybranej grupy wybierz zakładkę **Zasady**.
3. Z menu kontekstowego listy profili wybierz **Widok** → **Zasady dziedziczone**.

Profile dziedziczone zostaną wyświetlone na liście profili z następującą ikoną:

-  — jeśli były dziedziczone od grupy utworzonej na głównym Serwerze administracyjnym.
-  — jeśli były dziedziczone od grupy z wyższego poziomu hierarchii.

Jeżeli włączony jest tryb dziedziczenia ustawień, profile dziedziczone będą mogły być modyfikowane tylko w grupie, w której zostały utworzone. Modyfikowanie profili dziedziczonych nie jest możliwe w grupie, która je dziedziczy.

Aktywowanie profilu

W celu aktywowania profilu dla wybranej grupy:

1. W obszarze roboczym grupy, na zakładce **Zasady** wybierz profil, który chcesz aktywować.
2. W celu aktywowania profilu wykonaj jedno z następujących działań:
   - Z otwartego menu kontekstowego zasady wybierz **Zasada aktywna**.
   - W oknie właściwości profilu otwórz sekcję **Ogólny** i wybierz **Zasada aktywna** z grupy ustawień **Stan zasady**.

Profil stanie się aktywny dla wybranej grupy administracyjnej.

Podczas stosowania profilu do dużej liczby urządzeń klienckich, zarówno obciążenie Serwera administracyjnego, jak i ruch sieciowy zostają znacząco zwiększone na pewien czas.

Aktywowanie zasady automatycznie po wystąpieniu zdarzenia Epidemia wirusa

W celu skonfigurowania zasady tak, aby była aktywowana automatycznie po wystąpieniu Epidemii wirusa:

1. W oknie właściwości Serwera administracyjnego otwórz sekcję **Epidemia wirusa**.
2. Otwórz okno **Aktywacja zasady**, klikając odnośnik **Skonfiguruj zasady, które zostaną aktywowane po wystąpieniu epidemii wirusa** i dodając profil do wybranej listy profili aktywowanych po wystąpieniu epidemii wirusa.

Jeśli profil został aktywowany po wystąpieniu zdarzenia *Epidemia wirusa*, możesz wrócić do poprzedniego profilu tylko przy użyciu trybu ręcznego.

Stosowanie profilu użytkownika mobilnego

Profil użytkownika mobilnego jest aktywowany na urządzeniu w przypadku, gdy zostaje ono odłączone od sieci firmowej.

W celu zastosowania zasady użytkownika mobilnego:

W oknie właściwości profilu otwórz sekcję **Ogólny** i w grupie ustawień **Stan zasady** wybierz **Zasada użytkownika mobilnego**.

Zasada użytkownika mobilnego zostanie zastosowana na urządzeniach, jeśli są odłączone od sieci firmowej.

Modyfikowanie profilu. Wycofywanie zmian

W celu zmodyfikowania profilu:

1. Z drzewa konsoli wybierz folder **Zasady**.
2. W obszarze roboczym folderu **Zasady** wybierz profil i przejdź do okna właściwości profilu, korzystając z menu kontekstowego.
3. Wprowadź niezbędne zmiany.
4. Kliknij **Zastosuj**.

Zmiany wprowadzone w profilu zostaną zapisane we właściwościach profilu, w sekcji **Historia rewizji**.

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w profilu.

W celu wycofania zmian wprowadoznych w profilu:

1. Z drzewa konsoli wybierz folder **Zasady**.
2. Wybierz profil, w którym należy wycofać zmiany, i przejdź do okna właściwości profilu, korzystając z menu kontekstowego.
3. W oknie ustawień zasady wybierz sekcję **Historia rewizji**.
4. Na liście rewizji profilu wybierz numer rewizji, do której chcesz wycofać zmiany.
5. Kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz wartość **Wycofaj**.

Porównywanie profili

Dla jednej zarządzanej aplikacji możesz porównać dwa profile. Po zakończeniu porównywania, uzyskasz raport wyszczególniający te ustawienia, które są takie same, oraz te, które są różne. Może być, na przykład, konieczność porównania profili, jeśli różni administratorzy w swoich biurach utworzyli kilka profili dla jednej zarządzanej aplikacji lub jeśli profil najwyższego poziomu został odziedziczony przez wszystkie lokalne biura i został zmodyfikowany dla każdego biura. Profile można porównać w jeden z następujących sposobów: poprzez wybranie jednego profilu i porównanie go z innym lub poprzez porównanie dowolnych dwóch profili z listy profili.

W celu porównania jednego profilu z innym:

1. Z drzewa konsoli wybierz folder **Zasady**.
2. W obszarze roboczym folderu **Zasady** wybierz profil, który chcesz porównać z innym.
3. W menu kontekstowym zasady wybierz **Porównaj zasadę z inną zasadą**.
4. W oknie **Wybierz zasadę** wybierz profil, z którym ma być porównany Twój profil.
5. Kliknij **OK**.

Zostanie wyświetlony raport w formacie HTML z porównaniem dwóch profili dla tej samej aplikacji.

W celu porównania dwóch dowolnych profili z listy profili:

1. W folderze **Zasady**, na liście zasad użyj klawisza **`Shift`** lub **`Ctrl`**, aby wybrać dwie zasady dla jednej zarządzanej aplikacji.
2. Z menu kontekstowego wybierz **Porównaj**.

Zostanie wyświetlony raport w formacie HTML z porównaniem dwóch profili dla tej samej aplikacji.

Raport dotyczący porównania ustawień profilu dla Kaspersky Endpoint Security for Windows zawiera także szczegóły odnośnie porównania profili zasad. Możesz zminimalizować wyniki porównania profilu zasad. Aby zminimalizować sekcję, kliknij ikonę (▲) obok nazwy sekcji.

Usuwanie zasady

W celu usunięcia profilu:

1. W obszarze roboczym grupy administracyjnej, na zakładce **Zasady** wybierz profil, który chcesz usunąć.
2. Usuń profil w jeden z następujących sposobów:
   - Wybierając **Usuń** z menu kontekstowego profilu.
   - Klikając odnośnik **Usuń zasadę** w oknie z informacjami dla wybranego profilu.

Kopiowanie zasady

W celu skopiowania profilu:

1. W obszarze roboczym żądanej grupy, na zakładce **Zasady** wybierz profil.
2. Z otwartego menu kontekstowego zasady wybierz **Kopiuj**.
3. W drzewie konsoli wybierz grupę, do której chcesz dodać profil.
   Możesz dodać profil do grupy, z której został skopiowany.
4. Z menu kontekstowego listy profili dla wybranej grupy, na zakładce **Zasady** wybierz **Wklej**.

Profil zostanie skopiowany ze wszystkimi swoimi ustawieniami i zastosowany na urządzeniach w obrębie grupy, do której został skopiowany. Jeżeli wkleisz profil do tej samej grupy, z której został skopiowany, do jego nazwy zostanie automatycznie dodany przyrostek **(<kolejny numer>)**, na przykład: **(1)**, **(2)**.

Podczas kopiowania aktywny profil staje się nieaktywny. W razie konieczności będzie można aktywować ten profil.

Eksportowanie profilu

W celu wyeksportowania profilu:

1. Wyeksportuj profil w jeden z następujących sposobów:
   - Wybierając **Wszystkie zadania** → **Eksportuj** z menu kontekstowego profilu.
   - Klikając odnośnik **Eksportuj zasadę do pliku** w oknie z informacjami dla wybranej zasady.
2. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę dostępu pliku profilu. Kliknij przycisk **Zapisz**.

Importowanie profilu

W celu zaimportowania profilu:

1. W obszarze roboczym żądanej grupy, na zakładce **Zasady** wybierz jeden z następujących sposobów importowania profili:
   - Wybierz **Wszystkie zadania** → **Importuj** z menu kontekstowego listy profili.
   - Kliknij przycisk **Importuj zasadę z pliku** w sekcji zarządzania listą profili.
2. W oknie, które zostanie otwarte, określ ścieżkę dostępu do pliku, z którego chcesz zaimportować profil. Kliknij przycisk **Otwórz**.

Zaimportowana polityka zostanie wyświetlona na liście zasad. Importowane są również ustawienia i profile zasad. Niezależnie od statusu zasady, który został wybrany podczas eksportu, importowana zasada jest nieaktywna. Możesz zmienić stan zasady we właściwościach zasady.

Jeżeli nowo importowana zasada ma nazwę identyczną z nazwą istniejącej zasady, nazwa importowanej zasady jest rozszerzana o indeks **(<następny numer kolejny>)**, na przykład: **(1)**, **(2)**.

Konwertowanie profili

Kaspersky Security Center może konwertować polityki z wcześniejszych wersji zarządzanych aplikacji firmy Kaspersky na aktualne wersje tych samych aplikacji. Przekonwertowane zasady zachowują ustawienia aktualnego administratora sprzed aktualizacji, jak również zawierają nowe ustawienia z aktualnych wersji aplikacji. Wtyczki zarządzające dla aplikacji firmy Kaspersky określają, czy konwersja jest dostępna dla profili tych aplikacji. Aby uzyskać informacje na temat konwertowania profili dla każdej obsługiwanej aplikacji firmy Kaspersky, zapoznaj się z odpowiednią Pomocą z poniższej listy:

- **Aplikacje Kaspersky dla stacji roboczych:**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux Elbrus Edition
  - Kaspersky Endpoint Security for Linux ARM Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security for Windows
- **Kaspersky Industrial CyberSecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (scentralizowana zdalna instalacja nie jest obsługiwana)
- **Aplikacje firmy Kaspersky na urządzenia mobilne:**
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS
- **Aplikacje Kaspersky dla serwerów plików:**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
- **Aplikacje Kaspersky dla maszyn wirtualnych:**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless
- **Aplikacje Kaspersky dla systemów pocztowych i serwerów SharePoint / współpracy:**
  - Kaspersky Security for Linux Mail Server
  - Kaspersky Secure Mail Gateway

- Kaspersky Security for Microsoft Exchange Servers

- **Aplikacje kaspersky do wykrywania ataków ukierunkowanych:**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **Aplikacje firmy Kaspersky na urządzenia KasperskyOS:**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (wtyczka do Kaspersky Thin Client)

W celu konwertowania profili:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz skonwertować zasady.
2. W menu kontekstowym Serwera administracyjnego wybierz **Wszystkie zadania → Kreator konwersji zasad i zadań**.

Zostanie uruchomiony Kreator konwersji zasad i zadań. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu pracy kreatora tworzone są nowe zasady, które wykorzystują ustawienia zasad bieżącego administratora oraz nowe ustawienia z aktualnych wersji aplikacji firmy Kaspersky.

Zarządzanie profilami zasad

Ta sekcja opisuje zarządzanie profilami zasad i zawiera informacje o wyświetlaniu profili zasad, zmienianiu priorytetu profili zasad, tworzeniu profili zasad, modyfikowaniu profili zasad, kopiowaniu profili zasad, tworzeniu reguł aktywacji profili zasad i usuwaniu profili zasad.

Informacje o profilu zasad

Profil zasad to zestaw ustawień zasady, która jest aktywowana na urządzeniu klienckim (komputerze lub urządzeniu mobilnym), gdy urządzenie spełnia określone reguły aktywacji. Aktywacja profilu zmodyfikuje ustawienia zasad, które były aktywne na urządzeniu przed aktywacją profilu. Te ustawienia przyjmują wartości określone w profilu.

Profile zasad są niezbędne dla urządzeń w jednej grupie administracyjnej w celu uruchomienia z ustawieniami innych zasad. Taka sytuacja może mieć miejsce, na przykład, gdy ustawienia zasad muszą zostać zmodyfikowane dla niektórych urządzeń w grupie administracyjnej. W tym przypadku możesz skonfigurować profile zasad dla takiej zasady, co umożliwi zmodyfikowanie ustawień zasady dla wybranych urządzeń w grupie administracyjnej. Na przykład, zasada zabrania uruchamiania programu do nawigacji GPS na wszystkich urządzeniach w grupie Zarządzanie użytkownikami. Program do nawigacji GPS jest wymagany tylko na jednym urządzeniu w grupie Zarządzanie użytkownikami — na urządzeniu, które należy do użytkownika zatrudnionego w charakterze kuriera. Możesz oznaczyć to urządzenie jako „Kurier" i ponownie skonfigurować profil zasad, aby uruchamianie programu do nawigacji GPS możliwe było tylko na urządzeniu oznaczonym jako „Kurier", zachowując przy tym wszystkie pozostałe ustawienia zasady. W tym przypadku, jeśli urządzenie oznaczone jako „Kurier" pojawi się w grupie Zarządzanie użytkownikami, będzie można uruchamiać na nim program do nawigacji GPS. Uruchamianie programu do nawigacji GPS wciąż będzie zabronione na innych urządzeniach w grupie Zarządzanie użytkownikami do momentu oznakowania ich jako „Kurier".

Profile są obsługiwane tylko przez następujące zasady:

- Zasady Kaspersky Endpoint Security for Windows
- Zasady Kaspersky Endpoint Security for Mac
- Zasady wtyczki Kaspersky Mobile Device Management od wersji 10 Service Pack 1 do wersji 10 Service Pack 3 Maintenance Release 1
- Zasady wtyczki Kaspersky Device Management for iOS
- Zasady Kaspersky Security for Virtualization 5.1 Light Agent for Windows
- Zasady Kaspersky Security for Virtualization 5.1 Light Agent for Linux

Profile zasad upraszczają zarządzanie urządzeniami klienckimi, do których stosowane są zasady:

- Ustawienia profilu zasad mogą różnić się od ustawień zasady.
- Nie jest konieczne posiadanie i ręczne stosowanie kilku instancji jednej zasady, która różni się tylko kilkoma ustawieniami.
- Nie jest konieczne przydzielanie oddzielnej zasady do użytkowników mobilnych.
- Możesz wyeksportować lub zaimportować profile zasad, a także utworzyć nowe profile zasad w oparciu o istniejące profile.
- Jedna zasada może posiadać kilka aktywnych profili zasad. Tylko profile spełniające wymagania reguł aktywacji na urządzeniu zostaną zastosowane do tego urządzenia.
- Profile podlegają hierarchii zasad. Odziedziczona zasada zawiera wszystkie profile zasady wyższego poziomu.

Priorytety profili

Profile, które zostały utworzone dla zasad, są sortowane w kolejności malejącej priorytetu. Na przykład, jeśli profil X jest wyżej na liście profili niż profil Y, profil X posiada wyższy priorytet niż Y. Do jednego urządzenia można podłączyć kilka profili jednocześnie. Jeśli wartości ustawień różnią się w innych profilach, na urządzeniu zostanie zastosowana wartość z profilu najwyższego poziomu.

Reguły aktywacji profili

Profil zasad jest aktywowany na urządzeniu klienckim po wyzwoleniu reguły aktywacji. *Reguły aktywacji* to zestaw warunków, które, gdy zostaną spełnione, uruchamiają profil zasad na urządzeniu. Reguła aktywacji może zawierać następujące warunki:

- Agent sieciowy na urządzeniu klienckim łączy się z Serwerem administracyjnym przy użyciu określonego zestawu ustawień połączenia, takich jak adres Serwera administracyjnego, numer portu itd.
- Urządzenie klienckie jest offline.
- Do urządzenia klienckiego przypisano określone znaczniki.
- Urządzenia klienckie są jawnie (urządzenie jest natychmiast umieszczane w określonej jednostce) lub niejawnie (urządzenie jest umieszczane w jednostce, która znajduje się w określonej jednostce na dowolnym poziomie

zagnieżdżenia) umieszczane w określonej jednostce Active Directory®, urządzenie lub jego właściciel znajduje się w grupie zabezpieczeń Active Directory.

- To urządzenie klienckie należy do określonego użytkownika lub właściciel urządzenia należy do wewnętrznej grupy bezpieczeństwa Kaspersky Security Center.
- Właścicielowi urządzenia klienckiego została przypisana określona rola.

Zasady w hierarchii grup administracyjnych

Jeśli tworzysz zasadę w grupie administracyjnej niskiego poziomu, ta nowa zasada odziedziczy wszystkie profile aktywnej zasady z grupy wyższego poziomu. Profile z identycznymi nazwami zostają scalone. Profile zasad dla grupy wyższego poziomu posiadają wyższy priorytet. Na przykład, w grupie administracyjnej *A*, zasada *P(A)* posiada profile *X1*, *X2* i *X3* (w kolejności malejącej priorytetu). W grupie administracyjnej *B*, która jest podgrupą grupy *A*, zasada *P(B)* została utworzona z profilami *X2*, *X4*, *X5*. Następnie zasada *P(B)* zostanie zmodyfikowana przez zasadę *P(A)*, co spowoduje, że lista profili zasady *P(B)* będzie wyglądać następująco: *X1*, *X2*, *X3*, *X4*, *X5* (w kolejności malejącej priorytetu). Priorytet profilu *X2* będzie zależał od początkowego stanu *X2* zasady *P(B)* i *X2* zasady *P(A)*. Po utworzeniu zasady *P(B)*, zasada *P(A)* nie będzie już wyświetlana w podgrupie *B*.

Aktywna zasada jest ponownie wyliczana za każdym razem, gdy uruchamiany jest Agent sieciowy, włączany i wyłączany jest tryb offline lub modyfikowana jest lista znaczników przydzielonych do urządzenia klienckiego. Na przykład, rozmiar pamięci RAM został zwiększony na urządzeniu, co spowodowało aktywowanie profilu zasad stosowanego na urządzeniach posiadających dużą ilość pamięci RAM.

Właściwości i ograniczenia profili zasad

Profile posiadają następujące właściwości:

- Profile nieaktywnej zasady nie mają wpływu na urządzenia klienckie.
- Jeśli dla zasady ustawiono stan **Zasada użytkownika mobilnego**, profile zasad będą także stosowane tylko wtedy, gdy urządzenie jest odłączone od sieci firmowej.
- Profile nie obsługują statycznej analizy dostępu do plików wykonywalnych.
- Profil zasad nie może zawierać żadnych ustawień powiadomień o zdarzeniach.
- Jeśli port UDP o numerze 15000 jest używany do łączenia urządzenia z Serwerem administracyjnym, w ciągu minuty od przydzielenia znacznika do urządzenia zostaje aktywowany odpowiedni profil zasad.
- Podczas tworzenia reguł aktywacji profilu zasad możesz korzystać z reguł dla połączenia Agenta sieciowego z Serwerem administracyjnym.

Tworzenie profilu zasad

Tworzenie profilu jest dostępne tylko dla zasad następujących aplikacji:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows i nowsze wersje
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac

- Wtyczka Kaspersky Mobile Device Management w wersji 10 Service Pack 1 do wersji 10 Service Pack 3 Maintenance Release 1
- Wtyczka Kaspersky Device Management for iOS
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows i Linux

W celu utworzenia profilu zasad:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której profilu chcesz utworzyć profil zasad.
2. W obszarze roboczym grupy administracyjnej wybierz zakładkę **Zasady**.
3. Wybierz profil i przejdź do okna właściwości profilu, korzystając z menu kontekstowego.
4. Otwórz sekcję **Profile zasad** w oknie właściwości zasady, a następnie kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator nowego profilu zasad.
5. W oknie **Nazwa profilu zasad** określ następujące elementy:

   a. Nazwa profilu zasad

      Nazwa profilu nie może zawierać więcej niż 100 znaków.

   b. Stan profilu zasad (*Włączony* lub *Wyłączony*)

      Zalecamy utworzenie i włączenie nieaktywnych profili zasad dopiero po całkowitym zakończeniu pracy z ustawieniami i warunkami aktywacji profilu zasad.
6. Zaznacz pole **Po zamknięciu kreatora tworzenia nowej zasady, przejdź do konfiguracji reguły aktywacji profilu zasad**, aby uruchomić Kreator reguły aktywacji nowego profilu zasad. Postępuj zgodnie z instrukcjami kreatora.
7. Zmodyfikuj ustawienia profilu zasad w oknie właściwości profilu zasad w wybrany przez siebie sposób.
8. Zapisz zmiany, klikając **OK**.

   Profil zostanie zapisany. Profil zostanie aktywowany na urządzeniach, które spełniają warunki reguły aktywacji.

Dla jednej zasady można utworzyć kilka profili. Profile utworzone dla profilu są wyświetlane we właściwościach profilu, w sekcji **Profile zasad**. Możesz zmienić profil zasad i zmienić priorytet profilu, a także usunąć profil.

Modyfikowanie profilu zasad

Modyfikowanie ustawień profilu zasad

Możliwość modyfikowania profilu zasad jest dostępna tylko dla profili Kaspersky Endpoint Security for Windows.

W celu zmodyfikowania profilu zasad:

1. W drzewie konsoli wybierz grupę administracyjną, dla której powinien zostać zmodyfikowany profil zasad.

2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.
3. Wybierz profil i przejdź do okna właściwości profilu, korzystając z menu kontekstowego.
4. We właściwościach profilu otwórz sekcję **Profile zasad**.

   Ta sekcja zawiera listę profili, które zostały utworzone dla zasad. Profile są wyświetlane na liście zgodnie z ich priorytetami.
5. Wybierz profil zasad i kliknij przycisk **Właściwości**.
6. Skonfiguruj profil w oknie właściwości:
   - Jeśli jest to konieczne, w sekcji **Ogólny** zmień nazwę profilu i włącz lub wyłącz profil, korzystając z pola **Włącz profil**.
   - W sekcji **Reguły aktywacji** zmodyfikuj reguły aktywacji profilu.
   - Zmodyfikuj ustawienia profilu w odpowiednich sekcjach.
7. Kliknij **OK**.

Zmodyfikowane ustawienia zostaną zastosowane po zsynchronizowaniu urządzenia z Serwerem administracyjnym (jeśli profil zasad jest aktywny) lub po wyzwoleniu reguły aktywacji (jeśli profil zasad jest nieaktywny).

Zmiana priorytetu profilu zasad

Priorytety profili zasad definiują kolejność aktywacji profili na urządzeniu klienckim. Priorytety są używane, jeśli dla różnych profili zasad ustawiono identyczne reguły aktywacji.

Na przykład utworzono dwa profile zasad: *Profil 1* i *Profil 2*, które różnią się wartościami jednego ustawienia (*Wartość 1* i *Wartość 2*). Priorytet *Profilu 1* jest wyższy niż priorytet *Profilu 2*. Co więcej, istnieją także profile, których priorytety są niższe niż *Profilu 2*. Reguły aktywacji dla tych profili są identyczne.

Jeśli zostanie wyzwolona reguła aktywacji, *Profil 1* zostanie aktywowany. Ustawienie na urządzeniu przyjmie *Wartość 1*. Jeśli usuniesz *Profil 1*, wówczas *Profil 2* będzie miał najwyższy priorytet, a ustawienie przyjmie *Wartość 2*.

Na liście profili zasad profile są wyświetlane zgodnie z ich priorytetami. Profil o najwyższym priorytecie znajduje się na liście na pierwszym miejscu. Priorytet profilu można zmienić za pomocą przycisku strzałki w górę  i strzałki w dół  .

Usuwanie profilu zasad

W celu usunięcia profilu zasad:

1. W drzewie konsoli należy wybrać grupę administracyjną, której profil zasad chcesz usunąć.
2. W obszarze roboczym grupy administracyjnej wybierz zakładkę **Zasady**.
3. Wybierz profil i przejdź do okna właściwości profilu, korzystając z menu kontekstowego.
4. Otwórz sekcję **Profile zasad** we właściwościach profilu Kaspersky Endpoint Security.
5. Wybierz profil zasad, który chcesz usunąć i kliknij przycisk **Usuń**.

Profil zasad zostanie usunięty. Stan Aktywny zostanie przydzielony innemu profilowi zasad, którego reguły aktywacji zostaną wyzwolone na urządzeniu, lub profilowi.

Tworzenie reguły aktywacji profilu zasad

W celu utworzenia reguły aktywacji profilu zasad:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz utworzyć regułę aktywacji profilu zasad.
2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.
3. Wybierz profil i przejdź do okna właściwości profilu, korzystając z menu kontekstowego.
4. W oknie właściwości profilu otwórz sekcję **Profile zasad**.
5. Wybierz profil zasad, dla którego chcesz utworzyć regułę aktywacji, i kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości profilu zasad.

   Jeśli lista profili zasad jest pusta, możesz utworzyć profil zasad.
6. Wybierz sekcję **Reguły aktywacji** i kliknij przycisk **Dodaj**.

   Zostanie uruchomiony kreator nowej reguły aktywacji profilu zasad.
7. W oknie **Reguły aktywacji profilu zasad** zaznacz pola obok warunków, które mają wpływać na aktywację tworzonego profilu zasad:

   - **Główne reguły dotyczące aktywacji profilu zasad**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od stanu trybu offline urządzenia, regułę połączenia z Serwerem administracyjnym, a także znaczniki przypisywane do urządzenia.

   - **Reguły dotyczące używania Active Directory**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od obecności urządzenia w jednostce organizacyjnej Active Directory (OU) lub członkostwa urządzenia (lub jego właściciela) w grupie zabezpieczeń Active Directory.

   - **Reguły dla określonego właściciela urządzenia**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od właściciela urządzenia.

   - **Reguły dla specyfikacji sprzętowej**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od ilości pamięci oraz liczby procesów logicznych.

   Liczba dodatkowych okien w kreatorze zależy od ustawień wybranych w tym kroku. Reguły aktywacji profili zasad można zmodyfikować w późniejszym czasie.

8. W oknie **Główne warunki** określ następujące ustawienia:

- W polu **Urządzenie jest w trybie offline**, na liście rozwijalnej określ warunek obecności urządzenia w sieci:
  - Tak

    Urządzenie jest w sieci zewnętrznej, co oznacza, że Serwer administracyjny nie jest dostępny.
  - Nie

    Urządzenie jest w sieci, więc Serwer administracyjny jest dostępny.
  - Nie wybrano wartości

    Kryterium nie będzie stosowane.
- W polu **Urządzenie znajduje się w określonej lokalizacji sieciowej** użyj listy rozwijalnej, aby skonfigurować aktywację profilu zasad, jeśli reguła połączenia z Serwerem administracyjnym jest wykonywana / nie jest wykonywana na tym urządzeniu:
  - Wykonane / Niewykonane

    Warunek aktywacji profilu zasad (czy reguła jest wykonywana).
  - Nazwa reguły

    Opis lokalizacji sieciowej urządzenia dla połączenia z Serwerem administracyjnym, którego warunki muszą być spełnione (lub nie muszą być spełnione) dla aktywacji profilu zasad.

    Opis lokalizacji sieciowej urządzeń dla połączenia z Serwerem administracyjnym może zostać utworzony lub skonfigurowany w regule przełączania Agenta sieciowego.

Okno **Główne warunki** jest wyświetlane, jeśli pole **Główne reguły dotyczące aktywacji profilu zasad** jest zaznaczone.

9. W oknie **Warunki używające znaczników** określ następujące ustawienia:

- Lista znaczników

  Na liście znaczników możesz określić regułę uwzględniania urządzenia w profilu zasad, zaznaczając pola obok odpowiednich znaczników.

  Możesz dodać nowe znaczniki do listy, wprowadzając je w polu nad listą i klikając przycisk **Dodaj**.

  Profil zasad obejmuje urządzenia z opisami zawierającymi wszystkie zaznaczone tagi. Jeśli pola nie są zaznaczone, kryterium nie jest stosowane. Domyślnie pola te nie są zaznaczone.
- Zastosuj do urządzeń bez określonych znaczników

Włącz tę opcje, jeśli musisz odwrócić wybór znaczników.

Jeśli ta opcja jest włączona, profil zasad obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników. Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

Domyślnie opcja ta jest wyłączona.

Okno **Warunki używające znaczników** jest wyświetlane, jeśli pole **Główne reguły dotyczące aktywacji profilu zasad** jest zaznaczone.

10. W oknie **Warunki zawierające Active Directory** określ następujące ustawienia:

- Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory

  Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, którego właściciel jest członkiem określonej grupy zabezpieczeń. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- Członkostwo urządzenia w grupie zabezpieczeń Active Directory

  Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- Alokacja urządzenia w jednostce organizacyjnej Active Directory

  Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, które jest uwzględnione w określonej jednostce organizacyjnej Active Directory. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane.

  Domyślnie opcja ta jest wyłączona.

Okno **Warunki zawierające Active Directory** jest wyświetlane, jeśli pole **Reguły dotyczące używania Active Directory** jest zaznaczone.

11. W oknie **Warunki zawierające właściciela urządzenia** określ następujące ustawienia:

- Właściciel urządzenia

  Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu zgodnie z jego właścicielem. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

  - Urządzenie należy do określonego właściciela (znak „=”).
  - Urządzenie nie należy do określonego właściciela (znak „#”).

    Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić właściciela urządzenia, gdy opcja jest włączona. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- Właściciel urządzenia należy do wewnętrznej grupy zabezpieczeń

Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według przynależności właściciela do wewnętrznej grupy zabezpieczeń Kaspersky Security Center. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

- Właściciel urządzenia jest członkiem określonej grupy bezpieczeństwa (znak „=").
- Właściciel urządzenia nie jest członkiem określonej grupy bezpieczeństwa (znak „#").

  Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić grupę zabezpieczeń Kaspersky Security Center. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Aktywuj profil zasad określoną rolą właściciela urządzenia**

  Wybierz te opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu w zależności od roli właściciela. Dodaj rolę ręcznie z listy istniejących ról.

  Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium.

Okno **Warunki zawierające właściciela urządzenia** zostanie otwarte, jeśli pole **Reguły dla określonego właściciela urządzenia** jest zaznaczone.

12. W oknie **Warunki zawierające specyfikacje sprzętowe** określ następujące ustawienia:

- **Rozmiar pamięci RAM, w MB**

  Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu według ilości pamięci RAM dostępnej na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:
  - Rozmiar pamięci RAM jest mniejszy niż określona wartość (znak „<").
  - Rozmiar pamięci RAM jest większy niż określona wartość (znak „>").

  Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić ilość pamięci RAM na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Liczba procesorów logicznych**

  Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według liczby procesorów logicznych na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:
  - Liczba procesorów logicznych na urządzeniu jest mniejsza niż lub równa określonej wartości (znak „<").
  - Liczba procesorów logicznych na urządzeniu jest większa niż lub równa określonej wartości (znak „>").

  Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić liczbę procesorów logicznych na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

Okno **Warunki zawierające specyfikacje sprzętowe** jest wyświetlane, jeśli pole **Reguły dla specyfikacji sprzętowej** jest zaznaczone.

13. W oknie **Nazwa reguły aktywacji profilu zasad**, w polu **Nazwa reguły** określ nazwę dla reguły.

Profil zostanie zapisany. Profil zostanie aktywowany na urządzeniu po wyzwoleniu reguł aktywacji.

Reguły aktywacji profilu zasad utworzone dla profilu będą wyświetlone we właściwościach profilu zasad, w sekcji **Reguły aktywacji**. Możesz zmodyfikować lub usunąć dowolną regułę aktywacji profilu zasad.

Jednocześnie może być wyzwolonych kilka reguł aktywacji.

Reguły przenoszenia urządzeń

Zalecane jest automatyczne przydzielanie urządzeń do grup administracyjnych za pośrednictwem *reguł przenoszenia urządzeń*. Reguła przenoszenia urządzeń składa się z trzech głównych części: nazwy, warunku wykonania (wyrażenie logiczne z atrybutami urządzenia) oraz docelowej grupy administracyjnej. Reguła przenosi urządzenie do docelowej grupy administracyjnej, jeśli atrybuty urządzenia spełniają warunek wykonania reguły.

Wszystkie reguły przenoszenia urządzeń posiadają priorytety. Serwer administracyjny sprawdza, czy atrybuty urządzenia spełniają warunek wykonania każdej reguły, w rosnącej kolejności priorytetów. Jeśli atrybuty urządzenia spełniają warunek wykonania reguły, urządzenie zostaje przeniesione do grupy docelowej, a przetwarzanie reguły zostanie zakończone dla tego urządzenia. Jeśli atrybuty urządzenia spełniają warunki kilku reguł, urządzenie zostanie przeniesione do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

Reguły przenoszenia urządzeń mogą być tworzone pośrednio. Na przykład, we właściwościach pakietu instalacyjnego lub zadania zdalnej instalacji możesz określić grupę administracyjną, do której urządzenie musi zostać przeniesione po zainstalowaniu na nim Agenta sieciowego. Reguły przenoszenia urządzeń mogą być tworzone także bezpośrednio przez administratora Kaspersky Security Center na liście reguł przenoszenia. Lista ta znajduje się w Konsoli administracyjnej, we właściwościach grupy **Urządzenia nieprzypisane**.

Domyślnie reguła przenoszenia urządzeń jest przeznaczona do jednorazowego, wstępnego przydzielenia urządzeń do grup administracyjnych. Reguła przenosi urządzenia z grupy **Urządzenia nieprzypisane** tylko raz. Jeśli urządzenie był już raz przeniesione przy użyciu tej reguły, reguła ta nie przeniesie go już nawet wtedy, gdy ręcznie przeniesiesz urządzenie z powrotem do grupy **Urządzenia nieprzypisane**. Jest to zalecany sposób stosowania reguł przenoszenia.

Możesz przenieść urządzenia, które już zostały przydzielone do niektórych grup administracyjnych. Aby to zrobić, we właściwościach reguły odznacz pole **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**.

Stosowanie reguł przenoszenia do urządzeń, które już zostały przydzielone do niektórych grup administracyjnych, znacząco zwiększa obciążenie na Serwerze administracyjnym.

Możesz utworzyć regułę przenoszenia, która będzie nieprzerwanie oddziaływać na jedno urządzenie.

Szczególnie zalecane jest unikanie ciągłego przenoszenia jednego urządzenia z jednej grupy do drugiej (na przykład, w celu zastosowania specjalnego profilu do tego urządzenia, uruchomienia specjalnego zadania grupowego lub zaktualizowania urządzenia poprzez punkt dystrybucji).

Takie scenariusze nie są obsługiwane ponieważ w bardzo dużym stopniu zwiększają obciążenie na Serwerze administracyjnym oraz ruch sieciowy. Te scenariusze doprowadzają też do konfliktu z zasadami działania Kaspersky Security Center (szczególnie w obszarze uprawnień dostępu, zdarzeń i raportów). Należy znaleźć inne rozwiązanie, na przykład, poprzez użycie profili zasad, zadań dla wyborów urządzeń, przydzielania Agentów sieciowych zgodnie ze standardowym scenariuszem itd.

Klonowanie reguł przenoszenia urządzeń

Jeśli musisz utworzyć kilka reguł przenoszenia urządzeń z podobnymi ustawieniami, możesz sklonować istniejącą regułę i zmienić ustawienia sklonowanej reguły. Na przykład, jest to przydatne, gdy musisz mieć kilka identycznych reguł przenoszenia urządzeń z różnymi zakresami adresów IP i grupami docelowymi.

W celu sklonowania reguły przenoszenia urządzeń:

1. Otwórz okno główne aplikacji.
2. W folderze **Urządzenia nieprzypisane** kliknij **Konfiguruj reguły**.

   Zostanie otwarte okno **Właściwości: Urządzenia nieprzypisane**.
3. W sekcji **Przenieś urządzenia** wybierz regułę przenoszenia urządzeń, którą chcesz sklonować.
4. Kliknij **Sklonuj regułę**.

   Klon wybranej reguły przenoszenia urządzeń zostanie dodany na końcu listy.

Nowa reguła zostanie utworzona ze stanem wyłączenia. Regułę można edytować i włączać w dowolnym momencie.

Kategoryzacja oprogramowania

Głównym narzędziem do monitorowania uruchomień aplikacji są *kategorie Kaspersky* (zwane dalej *Kategorie KL*). Kategorie KL umożliwiają administratorom Kaspersky Security Center uproszczenie obsługi kategoryzacji oprogramowania i zminimalizowanie ruchu sieciowego skierowanego do zarządzanych urządzeń.

Kategorie użytkownika powinny być tworzone tylko dla aplikacji, których nie można zaklasyfikować do żadnej z istniejących kategorii KL (na przykład, dla oprogramowania wykonanego na zamówienie użytkownika). Kategorie użytkownika są tworzone na podstawie pakietu instalacyjnego aplikacji (MSI) lub folderu z pakietami instalacyjnymi.

Jeśli dostępna jest duża ilość programów, które nie zostały skategoryzowane poprzez kategorie KL, można utworzyć automatycznie aktualizowaną kategorię. Sumy kontrolne plików wykonywalnych będą automatycznie dodawane do tej kategorii po każdej modyfikacji folderu zawierającego pakiety dystrybucyjne.

Automatycznie aktualizowanych kategorii oprogramowania nie można tworzyć na podstawie folderów Moje dokumenty, %windir% oraz %ProgramFiles%. Pula plików w tych folderach podlega częstym zmianom, co prowadzi do zwiększonego obciążenia na Serwerze administracyjnym i zwiększonego ruchu sieciowego. Należy utworzyć dedykowany folder ze zbiorem oprogramowania i okresowo dodawać do niego nowe elementy.

Wymagania wstępne do zainstalowania aplikacji na urządzeniach w organizacji klienta

Proces zdalnej instalacji aplikacji na urządzeniach w organizacji klienta jest taki sam, jak proces zdalnej instalacji w obrębie korporacji.

W celu zainstalowania aplikacji na urządzeniach w organizacji klienta, należy wykonać następujące działania:

- Przed pierwszą instalacją aplikacji na urządzeniach w organizacji klienta zainstaluj na nich Agenta sieciowego.

  Przy konfigurowaniu pakietu instalacyjnego Agenta sieciowego przez dostawcę usługi w Kaspersky Security Center, należy dostosować następujące ustawienia w oknie właściwości pakietu instalacyjnego:

  - W sekcji **Połączenie**, w wierszu **Serwer administracyjny** określ adres tego samego wirtualnego Serwera administracyjnego, który określono w punkcie dystrybucji podczas lokalnej instalacji Agenta sieciowego.
  - W sekcji **Zaawansowane** zaznacz pole **Połącz z Serwerem administracyjnym korzystając z bramy połączenia**. W wierszu **Adres bramy połączenia** określ adres punktu dystrybucji. Można użyć adresu IP lub nazwy urządzenia w sieci Windows.

- Wybierz **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji** jako metodę pobierania dla pakietu instalacyjnego Agenta sieciowego. Metodę pobierania można wybrać w następujący sposób:

  - Jeśli instalujesz aplikację, korzystając z zadania zdalnej instalacji, możesz określić metodę w jeden z następujących sposobów:

    - Podczas tworzenia zadania zdalnej instalacji w oknie **Ustawienia**
    - W oknie właściwości zadania zdalnej instalacji, w sekcji **Ustawienia**

  - Jeśli instalujesz aplikacje, korzystając z kreatora zdalnej instalacji, możesz wybrać metodę pobierania w oknie **Ustawienia** tego kreatora.

- Konto wykorzystywane przez punkt dystrybucji do autoryzacji musi mieć uprawnienia dostępu do zasobu Admin$ na wszystkich urządzeniach klienckich.

Przeglądanie i modyfikowanie lokalnych ustawień aplikacji

System administracyjny Kaspersky Security Center umożliwia zdalne zarządzanie lokalnymi ustawieniami aplikacji na urządzeniach z poziomu Konsoli administracyjnej.

Lokalne ustawienia aplikacji są ustawieniami aplikacji określonymi dla urządzenia. Możesz użyć Kaspersky Security Center do określenia lokalnych ustawień aplikacji na urządzeniach znajdujących się w grupach administracyjnych.

Szczegółowe opisy ustawień aplikacji firmy Kaspersky znajdują się w odpowiednich dokumentach.

W celu przejrzenia lub modyfikacji lokalnych ustawień aplikacji:

1. W obszarze roboczym grupy, do której należą żądane urządzenia, wybierz zakładkę **Urządzenia**.
2. W oknie właściwości urządzenia, w sekcji **Aplikacje** wybierz żądaną aplikację.

3. Otwórz okno właściwości aplikacji, klikając dwukrotnie nazwę aplikacji lub klikając przycisk **Właściwości**.

   Zostanie otwarte okno lokalnych ustawień wybranej aplikacji, w którym będziesz mógł je przeglądać i modyfikować.

Możesz zmienić wartości ustawień, których modyfikowanie nie zostało zablokowane przez profil grupowy (tzn. które nie są oznaczone ikoną kłódki (🔒) w profilu).

Aktualizowanie Kaspersky Security Center i zarządzanych aplikacji

Ta sekcja opisuje kroki, jakie musisz podjąć, aby zaktualizować Kaspersky Security Center i zarządzane aplikacje.

Scenariusz: Regularne aktualizowanie baz danych i aplikacji Kaspersky

Ta sekcja oferuje scenariusz regularnego aktualizowania baz danych, modułów i aplikacji firmy Kaspersky. Po zakończeniu Konfigurowania scenariusza ochrony sieci, musisz zachować niezawodność systemu ochrony, aby upewnić się, że Serwery administracyjne i zarządzane urządzenia są chronione przed różnymi zagrożeniami, w tym wirusami, atakami sieciowymi i atakami phishingowymi.

Aktualność ochrony sieci jest zapewniana przez regularne aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky
- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

Po zakończeniu tego scenariusza, możesz być pewny, że:

- Twoja sieć jest chroniona przez najaktualniejsze oprogramowanie firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające.
- Antywirusowe bazy danych i inne bazy danych Kaspersky krytyczne dla bezpieczeństwa sieci są zawsze aktualne.

Wymagania wstępne

Zarządzane urządzenia muszą mieć połączenie z Serwerem administracyjnym. Jeśli nie mają połączenia, rozważ ręczne zaktualizowanie baz danych, modułów i aplikacji Kaspersky lub bezpośrednio z serwerów aktualizacji Kaspersky.

Serwer administracyjny musi mieć połączenie z Internetem.

Przed rozpoczęciem upewnij się, że:

1. Wdrożono aplikacje zabezpieczające Kaspersky na zarządzanych urządzeniach zgodnie ze scenariuszem wdrażania aplikacji Kaspersky poprzez Kaspersky Security Center Web Console.

2. Utworzyłeś i skonfigurowałeś wszystkie wymagane profile, profile zasad i zadania zgodnie ze scenariuszem konfigurowania ochrony sieci.

3. Przydzieliłeś odpowiednią liczbę punktów dystrybucji zgodnie z liczbą zarządzanych urządzeń i topologią sieci.

Aktualizowanie baz danych i aplikacji Kaspersky odbywa się w etapach:

1. **Wybranie schematu aktualizacji**

   Istnieje kilka schematów, których możesz użyć do zainstalowania aktualizacji dla komponentów Kaspersky Security Center i aplikacji zabezpieczających. Wybierz schemat lub kilka schematów, które najlepiej spełniają wymagania Twojej sieci.

2. **Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego**

   To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Jeśli nie uruchamiałeś kreatora, utwórz zadanie teraz.

   To zadanie jest wymagane do pobrania uaktualnień z serwerów aktualizacji Kaspersky do repozytorium Serwera administracyjnego, a także do zaktualizowania baz danych i modułów Kaspersky dla aplikacji Kaspersky Security Center. Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

   Jeśli w Twojej sieci są przypisane punkty dystrybucji, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. W tym przypadku zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego
   - Kaspersky Security Center Web Console: Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego

3. **Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji (opcjonalne)**

   Domyślnie, uaktualnienia są pobierane do punktów dystrybucji z Serwera administracyjnego. Możesz skonfigurować Kaspersky Security Center do pobierania uaktualnień do punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky. Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.

   Jeśli do Twojej sieci są przypisane punkty dystrybucji i utworzone jest zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, punkty dystrybucji pobiorą uaktualnienia z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji
   - Kaspersky Security Center Web Console: Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji

4. **Konfigurowanie punktów dystrybucji**

   Jeśli w Twojej sieci są przypisane punkty dystrybucji, upewnij się, że opcja **Roześlij aktualizacje** jest włączona we właściwościach wszystkich wymaganych punktów dystrybucji. Jeśli ta opcja jest włączona dla punktu dystrybucji, urządzenia znajdujące się w obszarze punktu dystrybucji pobierają uaktualnienia z repozytorium Serwera administracyjnego.

   Jeśli chcesz, żeby zarządzane urządzenia pobierały uaktualnienia tylko z punktów dystrybucji, włącz opcję **Rozsyłaj pliki tylko poprzez punkty dystrybucji** w zasadzie Agenta sieciowego.

5. **Optymalizowanie procesu aktualizacji przy użyciu trybu offline pobierania uaktualnień lub plików diff (opcjonalne)**

   Możesz zoptymalizować proces aktualizacji przy użyciu trybu offline pobierania uaktualnień (włączone domyślnie) lub przy użyciu plików diff. Dla każdego segmentu sieci musisz wybrać, którą z tych dwóch funkcji włączyć, ponieważ nie mogą działać jednocześnie.

   Jeśli tryb offline pobierania uaktualnień jest włączony, Agent sieciowy pobierze wymagane uaktualnienia na zarządzane urządzenie po pobraniu uaktualnień do repozytorium Serwera administracyjnego, zanim aplikacja zabezpieczająca zażąda uaktualnień. Zwiększy to niezawodność procesu aktualizacji. Aby korzystać z tej funkcji, włącz opcję **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)** w zasadzie Agenta sieciowego.

   Jeśli nie używasz trybu offline pobierania uaktualnień, możesz zoptymalizować ruch sieciowy między Serwerem administracyjnym a zarządzanymi urządzeniami przy użyciu plików diff. Jeśli ta funkcja jest włączona, Serwer administracyjny lub punkt dystrybucji pobierze pliki diff zamiast całych plików baz danych lub modułów Kaspersky. Plik diff opisuje różnice między dwoma wersjami pliku bazy danych lub modułu programu. Dlatego też plik diff zajmuje mniej miejsca niż cały plik. Spowoduje to zmniejszenie ruchu sieciowego między Serwerem administracyjnym lub punktami dystrybucji a zarządzanymi urządzeniami. Aby użyć tej funkcji, włącz opcję **Pobierz pliki diff** we właściwościach zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i/lub zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

   Dostępne instrukcje:

   - Używanie plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky
   - Konsola administracyjna: Włączanie i wyłączanie trybu offline pobierania uaktualnień
   - Kaspersky Security Center Web Console: Włączanie i wyłączanie trybu offline pobierania uaktualnień

6. **Sprawdzanie pobranych uaktualnień (opcjonalne)**

   Przed zainstalowaniem pobranych uaktualnień możesz zweryfikować uaktualnienia poprzez zadanie *Weryfikacja uaktualnień*. To zadanie kolejno uruchamia zadania aktualizacji i zadania skanowania w poszukiwaniu złośliwego oprogramowania urządzeń, skonfigurowane poprzez ustawienia dla określonego zbioru urządzeń testowych. Po uzyskaniu wyników zadania, Serwer administracyjny uruchamia lub blokuje propagację aktualizacji na pozostałe urządzenia.

   Zadanie *Weryfikacja uaktualnień* jest wykonywane jako część zadania *Pobierz uaktualnienia do repozytorium serwera administracyjnego*. We właściwościach zadania *Pobierz uaktualnienia do repozytorium serwera administracyjnego* włącz opcję **Zweryfikuj uaktualnienia przed rozesłaniem** w konsoli administracyjnej lub opcję **Uruchom weryfikację aktualizacji** w Kaspersky Security Center Web Console.

   Dostępne instrukcje:

   - Konsola administracyjna: Weryfikowanie pobranych uaktualnień
   - Kaspersky Security Center Web Console: Weryfikowanie pobranych uaktualnień

7. **Zatwierdzanie i odrzucanie aktualizacji oprogramowania**

   Domyślnie pobrane uaktualnienia oprogramowania posiadają stan *Niezdefiniowane*. Możesz zmienić stan na *Zatwierdzone* lub *Odrzucone*. Zatwierdzone aktualizacje są zawsze instalowane. Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia. Niezdefiniowane aktualizacje mogą zostać zainstalowane tylko na Agencie sieciowym, a inne komponenty Kaspersky Security Center zgodnie z ustawieniami zasady Agenta sieciowego. Aktualizacje, dla których ustawiłeś stan *Odrzucone*, nie zostaną zainstalowane na urządzeniach. Jeśli odrzucona aktualizacja dla aplikacji zabezpieczającej została wcześniej zainstalowana, Kaspersky Security Center spróbuje odinstalować aktualizację ze wszystkich urządzeń. Aktualizacje dla komponentów Kaspersky Security Center nie mogą zostać odinstalowane.

   Dostępne instrukcje:

   - Konsola administracyjna: Zatwierdzanie i odrzucanie aktualizacji oprogramowania

- Kaspersky Security Center Web Console: Zatwierdzanie i odrzucanie aktualizacji oprogramowania

8. **Konfigurowanie automatycznej instalacji uaktualnień i poprawek dla komponentów Kaspersky Security Center**

   Pobrane aktualizacje i łaty dla Agenta sieciowego i innych komponentów Kaspersky Security Center są instalowane automatycznie. Jeśli pozostawiłeś opcję **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany** włączoną we właściwościach Agenta sieciowego, wówczas wszystkie uaktualnienia zostaną zainstalowane automatycznie po ich pobraniu do repozytorium (lub kilku repozytoriów). Jeśli ta opcja jest wyłączona, poprawki Kaspersky, które zostały pobrane i oznaczone jako *Niezdefiniowane*, zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzone*.

   Dostępne instrukcje:

   - Konsola administracyjna: Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center
   - Kaspersky Security Center Web Console: Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center

9. **Instalacja uaktualnień dla Serwera administracyjnego**

   Aktualizacje oprogramowania dla Serwera administracyjnego nie zależą od stanów aktualizacji. Nie są instalowane automatycznie i muszą być wcześniej zatwierdzone przez administratora na zakładce **Monitorowanie** w Konsoli administracyjnej (**Serwer administracyjny** `<nazwa serwera>` → **Monitorowanie**) lub w sekcji **Powiadomienia** w Kaspersky Security Center Web Console (**Monitorowanie i raportowanie** → **Powiadomienia**). Następnie administrator musi wyraźnie uruchomić instalację uaktualnień.

10. **Konfigurowanie automatycznej instalacji uaktualnień dla aplikacji zabezpieczających**

    Utwórz zadania *Aktualizacji* dla zarządzanych aplikacji, aby zapewnić najnowsze aktualizacje aplikacji, modułów oprogramowania i baz danych Kaspersky, w tym antywirusowych baz danych. Aby zapewnić terminowe aktualizacje, zalecamy wybranie opcji **Po pobraniu nowych aktualizacji do repozytorium** podczas konfigurowania terminarza zadań.

    Jeśli Twoja sieć zawiera urządzenia obsługujące tylko protokół IPv6 i chcesz regularnie aktualizować aplikacje zabezpieczające zainstalowane na tych urządzeniach, upewnij się, że na zarządzanych urządzeniach zainstalowany jest Serwer administracyjny (w wersji nie wcześniejszej niż 13.2) oraz Agent sieciowy (w wersji nie wcześniejszej niż 13.2).

    Domyślnie, uaktualnienia dla Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Security for Linux są instalowane dopiero po zmianie stanu aktualizacji na *Zatwierdzone*. Ustawienia aktualizacji można zmienić w zadaniu *Aktualizacja*.

    Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia.

    Dostępne instrukcje:

    - Konsola administracyjna: Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach
    - Kaspersky Security Center Web Console: Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach

Wyniki

Po zakończeniu scenariusza, Kaspersky Security Center jest konfigurowany do aktualizowania baz danych Kaspersky i zainstalowanych aplikacji Kaspersky po pobraniu uaktualnień do repozytorium Serwera administracyjnego lub do repozytoriów punktów dystrybucji. Możesz przejść do monitorowania stanu sieci.

Informacje o aktualizowaniu baz danych, modułów i aplikacji Kaspersky

W celu upewnienia się, że ochrona Serwerów administracyjnych i zarządzanych urządzeń jest aktualna, w odpowiednim czasie należy dostarczać aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky

  Przed pobraniem baz danych i modułów oprogramowania Kaspersky oprogramowanie Kaspersky Security Center sprawdza, czy serwery Kaspersky są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić aktualizację antywirusowych baz danych oraz zachować poziom bezpieczeństwa zarządzanych urządzeń.

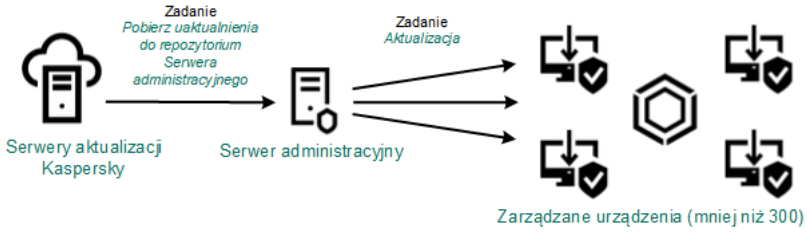
- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

W zależności od konfiguracji sieci, możesz użyć następujących schematów pobierania i rozsyłania żądanych aktualizacji na zarządzane urządzenia:

- Za pomocą jednego zadania: *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
- Używanie dwóch zadań:
  - Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
  - Zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*
- Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP
- Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach
- Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Używanie zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego

W tym schemacie Kaspersky Security Center pobiera aktualizacje za pośrednictwem zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. W małych sieciach, które zawierają mniej niż 300 zarządzanych urządzeń w jednym segmencie sieci lub mniej niż 10 zarządzanych urządzeń w każdym segmencie sieci, aktualizacje są rozsyłane na zarządzane urządzenia bezpośrednio z repozytorium Serwera administracyjnego (patrz rysunek poniżej).

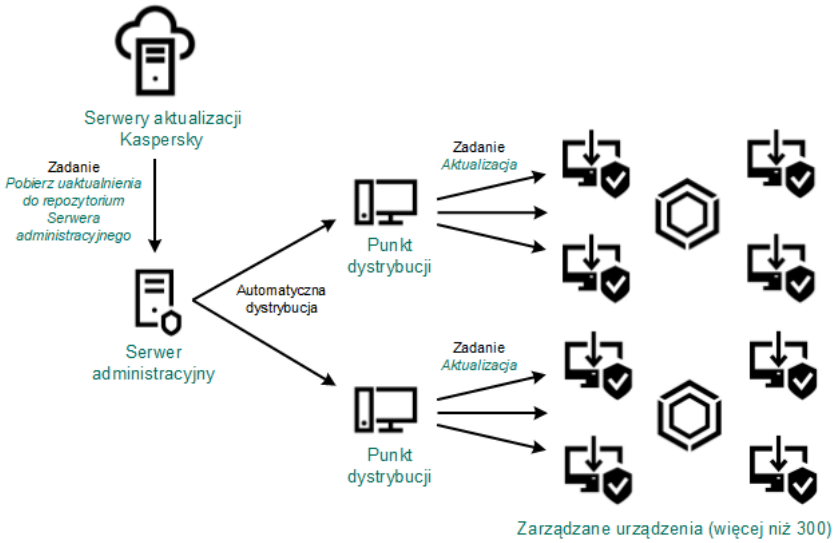


Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego bez punktów dystrybucji

Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

Jeśli sieć zawiera ponad 300 zarządzanych urządzeń w jednym segmencie sieci lub jeśli sieć zawiera kilka segmentów sieci z ponad 9 zarządzanymi urządzeniami w każdym segmencie sieci, zalecane jest użycie punktów dystrybucji do przesyłania aktualizacji na zarządzane urządzenia (patrz rysunek poniżej). Punkty dystrybucji zmniejszają obciążenie na Serwerze administracyjnym i optymalizują ruch sieciowy między Serwerem administracyjnym i zarządzanymi urządzeniami. Możesz obliczyć liczbę i konfigurację punktów dystrybucji wymaganych dla Twojej sieci.

W tym schemacie, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. Zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.



Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego z punktami dystrybucji

Jeśli zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* zostało zakończone, z repozytorium Serwera administracyjnego zostają pobrane następujące aktualizacje:

- Bazy danych i moduły Kaspersky dla Kaspersky Security Center

  Te aktualizacje są instalowane automatycznie.

- Bazy danych i moduły Kaspersky dla aplikacji zabezpieczających na zarządzanych urządzeniach

  Te aktualizacje są instalowane poprzez zadanie Aktualizacja dla Kaspersky Endpoint Security for Windows.

- Aktualizacje dla Serwera administracyjnego

  Te aktualizacje nie są instalowane automatycznie. Administrator musi wyraźnie zatwierdzić i uruchomić instalację aktualizacji.

  Uprawnienia lokalnego administratora są wymagane do zainstalowania łat na Serwerze administracyjnym.

- Aktualizacje dla komponentów Kaspersky Security Center

  Domyślnie, te aktualizacje są instalowane automatycznie. Możesz zmienić ustawienia w profilu Agenta sieciowego.

- Aktualizacje dla aplikacji zabezpieczających

  Domyślnie, Kaspersky Endpoint Security for Windows zainstaluje tylko te aktualizacje, które zatwierdzisz (aktualizacje możesz zatwierdzić za pośrednictwem Konsoli administracyjnej lub za pośrednictwem konsoli Kaspersky Security Center Web Console). Aktualizacje są instalowane poprzez zadanie *Aktualizacja* i mogą zostać skonfigurowane we właściwościach tego zadania.

Zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego* nie jest dostępne na wirtualnych Serwerach administracyjnych. Repozytorium wirtualnego Serwera administracyjnego wyświetla uaktualnienia pobrane na główny Serwer administracyjny.

Możesz skonfigurować sprawdzanie aktualizacji pod kątem łatwości obsługi i błędów na zestawie urządzeń testowych. Jeśli weryfikacja zostanie zakończona pomyślnie, aktualizacje będą rozsyłane na inne zarządzane urządzenia.

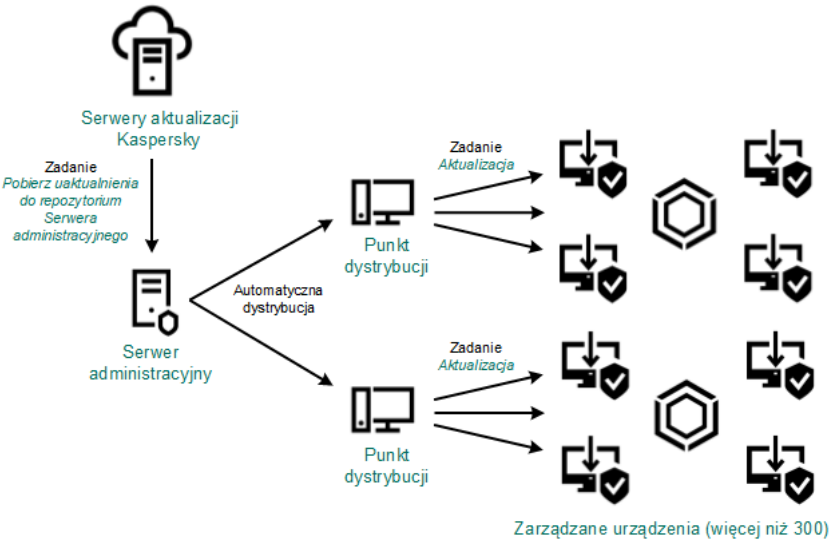
Każda aplikacja Kaspersky żąda wymaganych aktualizacji z Serwera administracyjnego. Serwer administracyjny gromadzi te żądania i pobiera tylko te uaktualnienia, które zostały zażądane przez aplikację. Dzięki temu te same uaktualnienia nie są pobierane kilka razy, a niepotrzebne uaktualnienia nie są pobierane wcale. Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, Serwer administracyjny automatycznie wysyła następujące informacje do serwerów aktualizacji Kaspersky w celu zapewnienia pobrania najnowszych wersji baz danych i modułów aplikacji Kaspersky:

- Identyfikator i wersja aplikacji
- Identyfikator instalacji aplikacji
- Identyfikator aktywnego klucza
- ID uruchamiania zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*

Żadna z przesyłanych informacji nie zawiera danych osobowych ani innych poufnych danych. Firma AO Kaspersky Lab chroni informacje zgodnie z wymogami wynikającymi z przepisów prawa.

Używanie dwóch zadań: zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego oraz zadanie Pobierz aktualizacje do repozytoriów punktów dystrybucji

Możesz pobrać aktualizacje do repozytoriów punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky zamiast repozytorium Serwera administracyjnego, a następnie rozesłać aktualizacje na zarządzane urządzenia (patrz rysunek poniżej). Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.



Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego oraz zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji

Domyślnie, Serwer administracyjny i punkty dystrybucji komunikują się z serwerami aktualizacji Kaspersky i pobierają uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny i/lub punkty dystrybucji do używania protokołu HTTP zamiast HTTPS.

Aby zaimplementować ten schemat, utwórz zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* jako dodatek do zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Po pobraniu przez punkty dystrybucji aktualizacji z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

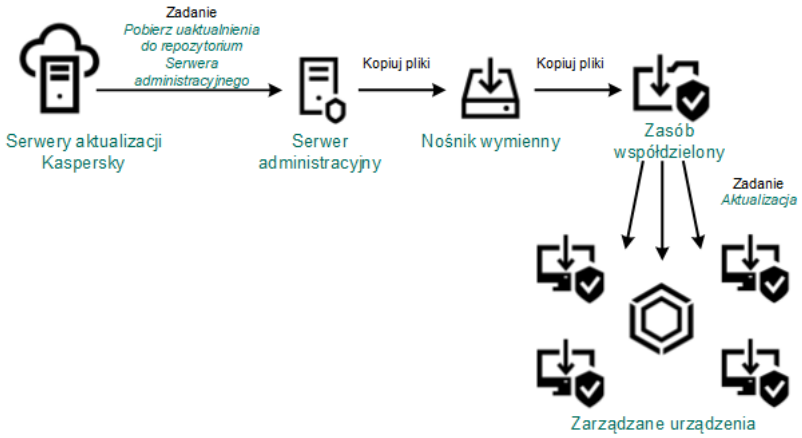
Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky.

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

Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* jest także wymagane dla tego schematu, ponieważ to zadanie jest używane do pobrania baz danych i modułów Kaspersky dla Kaspersky Security Center.

Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP

Jeśli urządzenia klienckie nie mają połączenia z Serwerem administracyjnym, możesz użyć folderu lokalnego lub zasobu współdzielonego jako źródła dla aktualizacji baz danych, modułów i aplikacji Kaspersky. W tym schemacie możesz skopiować wymagane aktualizacje z repozytorium Serwera administracyjnego na dysk wymienny, a następnie skopiować aktualizacje do folderu lokalnego lub zasobu współdzielonego, określonego jako źródło uaktualnień w ustawieniach Kaspersky Endpoint Security (patrz rysunek poniżej).



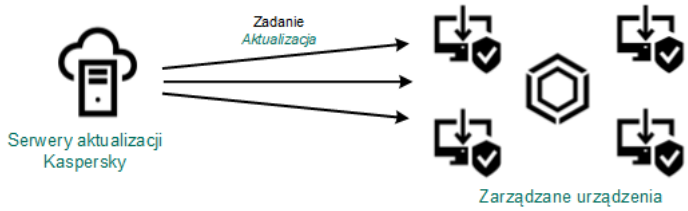
Aktualizowanie poprzez folder lokalny, folder współdzielony lub serwer FTP

Aby uzyskać więcej informacji na temat źródeł aktualizacji w Kaspersky Endpoint Security, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux — pomoc

Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach

Na zarządzanych urządzeniach możesz skonfigurować Kaspersky Endpoint Security w celu pobierania aktualizacji bezpośrednio z serwerów aktualizacji Kaspersky (patrz rysunek poniżej).



Aktualizowanie aplikacji zabezpieczających bezpośrednio z serwerów aktualizacji Kaspersky

W tym schemacie aplikacja zabezpieczająca nie używa repozytoriów dostarczonych przez Kaspersky Security Center. Aby pobierać uaktualnienia bezpośrednio z serwerów aktualizacji Kaspersky, określ serwery aktualizacji Kaspersky jako źródło uaktualnień w interfejsie aplikacji zabezpieczającej. Aby uzyskać więcej informacji na temat tych ustawień, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux — pomoc

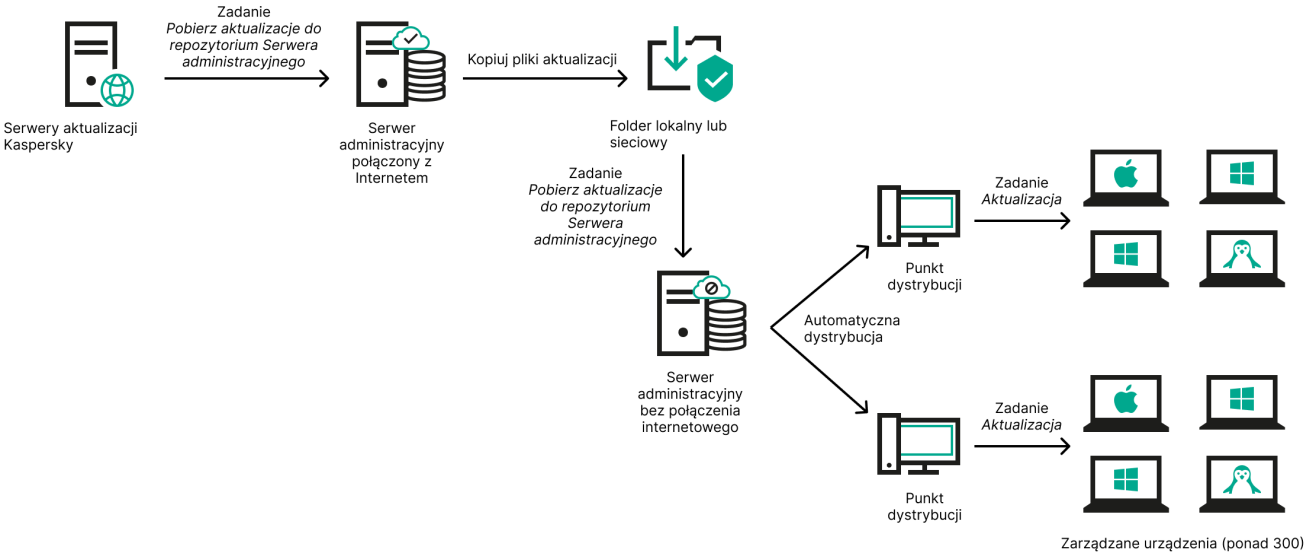
Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Jeżeli Serwer administracyjny nie ma połączenia z Internetem, możesz skonfigurować zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, aby pobierać uaktualnienia z folderu lokalnego lub sieciowego. W takim przypadku należy od czasu do czasu kopiować wymagane pliki aktualizacji do określonego folderu. Na przykład możesz skopiować wymagane pliki aktualizacji z jednego z następujących źródeł:

- Serwer administracyjny z połączeniem internetowym (patrz rysunek poniżej)

Ponieważ serwer administracyjny pobiera tylko aktualizacje wymagane przez aplikacje zabezpieczające, zestawy aplikacji zabezpieczających zarządzanych przez serwery administracyjne — ten, który ma połączenie z Internetem i ten, który go nie ma — muszą być zgodne.

Jeżeli Serwer administracyjny, którego używasz do pobierania uaktualnień, ma wersję 13.2 lub wcześniejszą, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.



Aktualizacja przez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

- Kaspersky Update Utility

  Ponieważ narzędzie to wykorzystuje stary schemat do pobierania uaktualnień, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.

Informacje o używaniu plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky

Jeśli Kaspersky Security Center pobiera uaktualnienia z serwerów aktualizacji Kaspersky, optymalizuje ruch sieciowy przy użyciu plików diff. Możesz także włączyć używanie plików diff przez urządzenia (Serwery administracyjne, punkty dystrybucji i urządzenia klienckie), które pobierają uaktualnienia z innych urządzeń w sieci.

Informacje o funkcji Pobierz pliki diff

Plik diff opisuje różnice między dwoma wersjami pliku bazy danych lub modułu programu. Użycie plików diff oszczędza ruch sieciowy w sieci firmowej, ponieważ pliki diff zajmują mniej miejsca niż całe pliki baz danych i modułów programu. Jeśli funkcja *Pobierz pliki diff* jest włączona na Serwerze administracyjnym lub w punkcie dystrybucji, pliki diff zostają zapisane na tym Serwerze administracyjnym lub w tym punkcie dystrybucji. W wyniku tego działania, urządzenia, które pobierają uaktualnienia z tego Serwera administracyjnego lub punktu dystrybucji, mogą używać zapisanych plików diff do aktualizacji swoich baz danych i modułów programu.

Aby zoptymalizować użycie plików diff, zalecana jest synchronizacja terminarza aktualizacji urządzeń z terminarzem aktualizacji Serwera administracyjnego lub punktu dystrybucji, z którego urządzenia pobierają uaktualnienia. Jednakże ruch sieciowy można oszczędzić nawet wtedy, gdy urządzenia są aktualizowane kilka razy rzadziej niż Serwer administracyjny lub punkt dystrybucji, z którego urządzenia pobierają uaktualnienia.

Funkcja Pobierz pliki diff może zostać włączona tylko na Serwerach administracyjnych i w punktach dystrybucji od wersji 11. Aby zapisać pliki diff na Serwerach administracyjnych i w punktach dystrybucji w wersjach wcześniejszych, zaktualizuj je do wersji 11 lub nowszej.

Funkcja Pobierz pliki diff jest niekompatybilna z trybem offline pobierania uaktualnień. Oznacza to, że Agenty sieciowe, które używają trybu offline pobierania uaktualnień nie pobierają plików diff nawet wtedy, gdy funkcja Pobierz pliki diff jest włączona na Serwerze administracyjnym lub w punkcie dystrybucji, który dostarcza uaktualnienia do tych Agentów sieciowych.

Punkty dystrybucji nie używają multiemisji IP do automatycznego rozsyłania plików diff.

Włączania funkcji Pobierz pliki diff: scenariusz

Wymagania wstępne

Wymagania wstępne scenariusza są następujące:

- Serwery administracyjne i punkty dystrybucji zostają zaktualizowane do wersji 11 lub nowszej.
- Tryb offline pobierania uaktualnień jest wyłączony w ustawieniach profilu Agenta sieciowego.

Etapy

1. **Włączanie funkcji na Serwerze administracyjnym**

   Włącz funkcję w ustawieniach zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego.

2. **Włączanie funkcji dla punktu dystrybucji**

   Włącz funkcję dla punktu dystrybucji, który pobiera uaktualnienia przy użyciu zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji.

   Następnie włącz funkcję dla punktu dystrybucji, który pobiera uaktualnienia z Serwera administracyjnego.

   Funkcja jest włączona w ustawieniach profilu Agenta sieciowego i—jeśli punkty dystrybucji są przypisywane ręcznie i jeśli chcesz zastąpić ustawienia profilu—w sekcji **Punkty dystrybucji** właściwości Serwera administracyjnego.

Aby sprawdzić, czy funkcja Pobierz pliki diff została pomyślnie włączona, możesz zmierzyć wewnętrzny ruch sieciowy przed i po wykonaniu scenariusza.

Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego

Zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego* jest automatycznie tworzone podczas działania kreatora wstępnej konfiguracji Kaspersky Security Center. Możesz utworzyć tylko jedno zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*. Dlatego też zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego* możesz utworzyć tylko wtedy, gdy takie zadanie zostało usunięte z listy zadań Serwera administracyjnego.

W celu utworzenia zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - W drzewie konsoli, z menu kontekstowego folderu **Zadania** wybierz **Nowe** → **Zadanie**.
   - W obszarze roboczym folderu **Zadania** kliknij przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. W oknie **Wybierz typ zadania** wybierz **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
4. W oknie **Ustawienia** określ ustawienia zadania w następujący sposób:
   - Źródła aktualizacji

     Jako źródła uaktualnień dla Serwera administracyjnego można użyć następujących zasobów:

     - Serwery aktualizacji Kaspersky

       Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji. Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

       Ta opcja jest wybrana domyślnie.

     - Główny Serwer administracyjny

       Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

     - Folder lokalny lub sieciowy

       Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

       Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

   - **Inne ustawienia**:
     - Wymuś aktualizację podrzędnych Serwerów administracyjnych

Jeżeli ta opcja jest włączona, Serwer administracyjny uruchomi zadania aktualizacji na podrzędnych Serwerach administracyjnych zaraz po pobraniu nowych aktualizacji. W innym przypadku zadania aktualizacji na podrzędnych Serwerach administracyjnych będą uruchamiane zgodnie ze swoimi terminarzami.

Domyślnie opcja ta jest wyłączona.

- Kopiuj pobrane aktualizacje do dodatkowych folderów

  Po otrzymaniu przez Serwer administracyjny uaktualnień skopiuje on je do określonych folderów. Użyj tej opcji, jeśli chcesz ręcznie zarządzać dystrybucją uaktualnień w sieci.

  Na przykład, chcesz użyć tej opcji w następującej sytuacji: sieć Twojej organizacji zawiera kilka niezależnych podsieci, a urządzenia z każdej podsieci nie mają dostępu do innych podsieci. Jednakże urządzenia we wszystkich podsieciach mają dostęp do wspólnego udziału sieciowego. W tym przypadku skonfiguruj Serwer administracyjny w jednej z podsieci tak, aby pobierał uaktualnienia z serwerów aktualizacji Kaspersky, włącz tę opcję, a następnie określ ten udział sieciowy. W zadaniach pobierania uaktualnień do repozytorium dla innych Serwerów administracyjnych określ ten sam udział sieciowy jako źródło uaktualnień.

  Domyślnie opcja ta jest wyłączona.

  - Nie wymuszaj aktualizacji urządzeń i podrzędnych Serwerów administracyjnych przed zakończeniem kopiowania

    Zadania pobierania aktualizacji na urządzenia klienckie i podrzędne Serwery administracyjne zostaną uruchomione dopiero po skopiowaniu aktualizacji z głównego folderu aktualizacji do dodatkowych folderów aktualizacji.

    Ta opcja musi być włączona, jeśli urządzenia klienckie i podrzędne Serwery administracyjne pobierają aktualizacje z dodatkowych folderów sieciowych.

    Domyślnie opcja ta jest wyłączona.

- Pobierz aktualizacje za pomocą starego schematu

Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

- Kaspersky Update Utility

  To narzędzie pobiera aktualizacje przy użyciu starego schematu.

- Kaspersky Security Center 13.2 lub wcześniejsza wersja

  Na przykład Twój serwer administracyjny 1 nie ma połączenia z Internetem. W takim przypadku możesz pobrać aktualizacje za pomocą serwera administracyjnego 2, który ma połączenie z Internetem, a następnie umieścić je w folderze lokalnym lub sieciowym, aby użyć go jako źródła uaktualnień dla serwera administracyjnego 1. Jeżeli serwer administracyjny 2 ma wersję 13.2 lub wcześniejszą, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu dla serwera administracyjnego 1.

Domyślnie opcja ta jest wyłączona.

5. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Zaplanowane uruchomienie:**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - **Co N godzin**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

  - **Co N dni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N tygodni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

    Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co N minut**

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po epidemii wirusa**

Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

- Ochrona antywirusowa stacji roboczych i serwerów plików
- Ochrona antywirusowa bram internetowych
- Ochrona antywirusowa serwerów pocztowych

Domyślnie, zaznaczone są wszystkie typy aplikacji.

Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest włączona.

- Używaj automatycznie losowego opóźnienia dla uruchamiania zadań

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

6. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

7. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

   Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu pracy kreatora, zadanie **Pobierz aktualizacje do repozytorium serwera administracyjnego** pojawi się na liście zadań Serwera administracyjnego w obszarze roboczym.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium serwera administracyjnego* Serwer administracyjny pobiera uaktualnienia baz danych i modułów programu ze źródła uaktualnień i przechowuje je w folderze współdzielonym Serwera administracyjnym. Jeśli tworzysz to zadanie dla grupy administracyjnej, zostanie ono zastosowane tylko do Agentów sieciowych umieszczonych w określonej grupie administracyjnej.

Uaktualnienia są rozsyłane do urządzeń klienckich i podrzędnych Serwerów administracyjnych z folderu współdzielonego Serwera administracyjnego.

Tworzenie zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji

Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky.

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

Możesz utworzyć zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* dla grupy administracyjnej. To zadanie będzie uruchamiane dla punktów dystrybucji znajdujących się w określonej grupie administracyjnej.

Możesz użyć tego zadania, na przykład, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktem(ami) dystrybucji jest droższy niż ruch sieciowy pomiędzy punktem(ami) dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.

W celu utworzenia zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji dla wybranej grupy administracyjnej:

1. Z drzewa konsoli wybierz folder **Zadania**.

2. W obszarze roboczym tego folderu kliknij przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

3. W oknie **Wybierz typ zadania** wybierz węzeł Serwer administracyjny **Kaspersky Security Center**, rozwiń folder **Zaawansowane**, a następnie wybierz zadanie **Pobierz aktualizacje do repozytoriów punktów dystrybucji**.

4. W oknie **Ustawienia** określ ustawienia zadania w następujący sposób:

   - Źródła aktualizacji

     Jako źródła uaktualnień dla punktu dystrybucji można użyć następujących zasobów:

     - Serwery aktualizacji Kaspersky

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

       Opcja ta jest wybrana domyślnie.

     - Główny Serwer administracyjny

       Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

     - Folder lokalny lub sieciowy

       Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

       Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

   - Folder do przechowywania aktualizacji

     Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

   - Pobierz aktualizacje za pomocą starego schematu

Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

- Kaspersky Update Utility

  To narzędzie pobiera aktualizacje przy użyciu starego schematu.

- Kaspersky Security Center 13.2 lub wcześniejsza wersja

  Na przykład punkt dystrybucji jest skonfigurowany do pobierania aktualizacji z folderu lokalnego lub sieciowego. W takim przypadku aktualizacje można pobrać za pomocą serwera administracyjnego z połączeniem internetowym, a następnie umieścić je w folderze lokalnym w punkcie dystrybucji. Jeśli serwer administracyjny ma wersję 13.2 lub wcześniejszą, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

Domyślnie opcja ta jest wyłączona.

5. W oknie **Wybierz Grupę administracyjną** kliknij **Przeglądaj** i wybierz grupę administracyjną, do której stosowane jest zadanie.

6. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

   - **Zaplanowane uruchomienie:**

     Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

     - **Co N godzin**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

       Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

     - **Co N dni**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

       Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

     - **Co N tygodni**

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- **Co N minut**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

  Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- Po epidemii wirusa

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest włączona.

- Używaj automatycznie losowego opóźnienia dla uruchamiania zadań

Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

7. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

8. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

   Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu pracy kreatora, zadanie **Pobierz aktualizacje do repozytoriów punktów dystrybucji** pojawi się na liście zadań Agenta sieciowego w docelowej grupie administracyjnej i w obszarze roboczym **Zadania** konsoli.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Po wykonaniu zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji*, aktualizacje baz danych i modułów aplikacji zostaną pobrane ze źródła uaktualnień i będą przechowywane w folderze współdzielonym. Pobrane uaktualnienia zostaną użyte tylko przez punkty dystrybucji, które znajdują się w określonej grupie administracyjnej i dla których nie ustawiono zadania pobierania uaktualnień.

W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Punkty dystrybucji**. We właściwościach każdego punktu dystrybucji, w sekcji **Źródło uaktualnień** możesz określić źródło uaktualnień (**Pobierz z Serwera administracyjnego** lub **Użyj zadania do wymuszonego pobierania uaktualnień**). Domyślnie, opcja **Pobierz z Serwera administracyjnego** jest wybrana dla punktu dystrybucji wskazanego ręcznie lub automatycznie. Te punkty dystrybucji będą używać wyników wykonania zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji*.

Właściwości każdego punktu dystrybucji określają folder sieciowy, który został utworzony osobno dla tego punktu dystrybucji. Nazwy folderów mogą być różne dla innych punktów dystrybucji. Dlatego też nie jest zalecane zmienianie nazwy folderu sieciowego we właściwościach zadania, jeśli zadanie jest tworzone dla grupy urządzeń.

Jeśli tworzysz zadanie lokalne dla urządzenia, możesz zmienić folder sieciowy z aktualizacjami we właściwościach zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji*.

Konfigurowanie zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego

W celu skonfigurowania zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego:

1. W obszarze roboczym folderu **Zadania**, z listy zadań wybierz **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.

2. Otwórz okno właściwości zadania w jeden z następujących sposobów:

   - Wybierając **Właściwości** w menu kontekstowym zadania.

   - Klikając odnośnik **Konfiguruj zadanie** w oknie z informacjami dla wybranego zadania.

   Zostanie otwarte okno właściwości zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*. W tym oknie możesz skonfigurować sposób pobierania uaktualnień do repozytorium Serwera administracyjnego.

Sprawdzanie pobranych uaktualnień

Przed zainstalowaniem aktualizacji na zarządzanych urządzeniach, w pierwszej kolejności możesz sprawdzić aktualizacje pod kątem łatwości obsługi i błędów poprzez zadanie *Weryfikacja uaktualnień*. Zadanie *Weryfikacja uaktualnień* jest wykonywane automatycznie jako część zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Serwer administracyjny pobierze uaktualnienia ze źródła, zapisze je w repozytorium tymczasowym i uruchomi *Weryfikacja uaktualnień*. Jeżeli zadanie zakończy się powodzeniem, uaktualnienia zostaną skopiowane z repozytorium tymczasowego do folderu współdzielonego na serwerze administracyjnym (<Folder instalacyjny Kaspersky Security Center>\Share\Updates). Zostaną one rozesłane do wszystkich urządzeń klienckich, dla których Serwer administracyjny jest źródłem uaktualnień.

Jeżeli zadanie *Weryfikacja uaktualnień* wykaże niepoprawność uaktualnień znajdujących się w repozytorium tymczasowym lub podczas wykonywania tego zadania wystąpi błąd, *Weryfikacja uaktualnień* nie zostaną skopiowane do folderu współdzielonego. Serwer administracyjny zachowa poprzedni zestaw uaktualnień. Zaplanowane zadania wykonywane zgodnie z opcją terminarza **Po pobraniu nowych uaktualnień do repozytorium** również nie zostaną uruchomione. Te działania są wykonywane podczas następnego uruchomienia zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, jeśli skanowanie nowych uaktualnień przebiegło bez problemów.

Zestaw uaktualnień jest uważany za nieprawidłowy, jeżeli przynajmniej na jednym urządzeniu testującym jest spełniony jeden z następujących warunków:

- Wystąpił błąd zadania aktualizacji.

- Stan ochrony w czasie rzeczywistym aplikacji zabezpieczającej zmienił się po zastosowaniu uaktualnień.

- W trakcie wykonywania zadania skanowania na żądanie wykryto zainfekowany obiekt.

- Wystąpił błąd w funkcjonowaniu programu firmy Kaspersky.

Jeśli żaden z powyższych warunków nie wystąpił na żadnym urządzeniu testującym, zestaw uaktualnień jest uważany za poprawny, a zadanie *Weryfikacja uaktualnień* uważa się za zakończone pomyślnie.

Zanim zaczniesz tworzyć zadanie *Weryfikacja uaktualnień*, zrealizuj wymagania wstępne:

1. Utwórz grupę administracyjną z kilkoma urządzeniami testowymi. Ta grupa będzie potrzebna do weryfikacji uaktualnień.

   Zaleca się korzystanie z urządzeń z najbardziej niezawodną ochroną i najpowszechniejszą konfiguracją aplikacji w całej sieci. Takie podejście zwiększa jakość i prawdopodobieństwo wykrycia wirusa podczas skanowania oraz minimalizuje ryzyko fałszywych alarmów. Jeśli na urządzeniach testujących zostaną wykryte wirusy, zadanie *weryfikacji uaktualnień* zakończy się niepowodzeniem.

2. Utwórz zadania aktualizacji i *Aktualizacja* w *Skanowanie w poszukiwaniu złośliwego oprogramowania* złośliwego oprogramowania do aplikacji obsługiwanej przez Kaspersky Security Center, na przykład Kaspersky Endpoint Security for Windows lub Kaspersky Security for Windows Server. Podczas tworzenia zadań *Aktualizacja* i *Skanowanie w poszukiwaniu złośliwego oprogramowania* określ grupę administracyjną z urządzeniami testowymi.

   Zadanie *Weryfikacja uaktualnień* uruchamia kolejno zadania *Aktualizacja* i *Skanowanie w poszukiwaniu złośliwego oprogramowania* na urządzeniach testowych, aby sprawdzić, czy wszystkie aktualizacje są prawidłowe. Ponadto podczas tworzenia zadania *Weryfikacja uaktualnień* musisz określić zadania *Aktualizacja* i *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

3. Utwórz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

W celu skonfigurowania Kaspersky Security Center do sprawdzania pobranych uaktualnień przed rozesłaniem ich na urządzenia klienckie:

1. W obszarze roboczym folderu **Zadania**, z listy zadań wybierz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

2. Otwórz okno właściwości zadania w jeden z następujących sposobów:

   - Wybierając **Właściwości** w menu kontekstowym zadania.

   - Klikając odnośnik **Konfiguruj zadanie** w oknie z informacjami dla wybranego zadania.

3. Jeśli zadanie weryfikacji *Weryfikacja uaktualnień* istnieje, kliknij przycisk **Przeglądaj**. W oknie, które zostanie otwarte, wybierz zadanie *Weryfikacja uaktualnień* w grupie administracyjnej z urządzeniami testowymi.

4. Jeśli wcześniej nie utworzono zadania *Weryfikacja uaktualnień*, kliknij przycisk **Utwórz**.

   Zostanie uruchomiony Kreator zadania *Weryfikacja uaktualnień*. Postępuj zgodnie z instrukcjami kreatora.

5. Kliknij **OK**, aby zamknąć okno właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*

Automatyczna weryfikacja uaktualnień zostanie włączona. Teraz możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnegoi*.

Konfigurowanie profili testowych i zadań pomocniczych

Podczas tworzenia zadania *weryfikacji uaktualnień* serwer administracyjny generuje profile testowe, pomocnicze grupowe zadania aktualizacji i zadania skanowania na żądanie.

Pomocnicze grupowe zadania aktualizacji i zadania skanowania na żądanie zajmują trochę czasu. Zadania te są wykonywane podczas wykonywania zadania *weryfikacji uaktualnień*. Zadanie *weryfikacji* uaktualnień jest wykonywane podczas wykonywania zadania *pobierania* aktualizacji do repozytorium. Czas trwania zadania *Pobierz uaktualnienia do repozytorium* obejmuje pomocnicze grupowe zadania aktualizacji i skanowania na żądanie.

Możesz zmodyfikować ustawienia profili testowych i zadań pomocniczych.

W celu zmodyfikowania ustawień profilu testowego lub zadania pomocniczego:

1. Z drzewa konsoli wybierz grupę, dla której tworzone jest zadanie *weryfikacji uaktualnień*.
2. W obszarze roboczym grupy wybierz jedną z następujących zakładek:
   - **Profile**, jeżeli chcesz zmodyfikować ustawienia profilu testowego.
   - **Zadania**, jeżeli chcesz zmienić ustawienia zadania pomocniczego.
3. Na zakładce obszaru roboczego wybierz profil lub zadanie, którego ustawienia chcesz zmodyfikować.
4. Otwórz okno właściwości profilu (zadania) w jeden z następujących sposobów:
   - Wybierając **Właściwości** z menu kontekstowego profilu (zadania).
   - Klikając odnośnik **Konfiguruj zasadę** (**Konfiguruj zadanie**) w oknie z informacjami dla wybranego profilu (zadania).

W celu sprawdzenia poprawności uaktualnień, na modyfikację ustawień profili testowych i zadań pomocniczych powinny zostać nałożone następujące ograniczenia:

- W ustawieniach zadania pomocniczego:
  - Zapisz wszystkie zadania z priorytetem **Zdarzenie krytyczne** i **Błąd funkcjonalny** na Serwerze administracyjnym. Przy użyciu tych typów zdarzeń Serwer administracyjny analizuje działanie aplikacji.
  - Użyj Serwera administracyjnego jako źródła uaktualnień.
  - Określ typ terminarza zadania: **Ręcznie**.
- W ustawieniach profili testowych:
  - Wyłącz technologie przyspieszające skanowanie iChecker i iSwift (**Podstawowa ochrona przed zagrożeniami → Ochrona plików → Ustawienia → Dodatkowe → Technologie skanowania**).
  - Wybierz działania na zainfekowanych obiektach: **Wylecz; usuń, jeśli leczenie nie powiedzie się** / **Wylecz; zablokuj, jeśli leczenie nie powiedzie się** / **Zablokuj** (**Podstawowa ochrona przed zagrożeniami → Ochrona plików → Akcja po wykryciu zagrożenia**).
- W ustawieniach profili testowych i zadań pomocniczych:

  Jeżeli po zainstalowaniu uaktualnień modułów oprogramowania konieczne jest ponowne uruchomienie urządzenia, należy to zrobić natychmiast. Jeżeli urządzenie nie zostanie uruchomione ponownie, niemożliwe będzie przetestowanie tego typu uaktualnień. Dla niektórych aplikacji instalacja uaktualnień wymagająca ponownego uruchomienia komputera może zostać zablokowana lub skonfigurowana tak, aby najpierw pytać użytkownika o potwierdzenie. Ograniczenia te powinny zostać wyłączone w ustawieniach profili testowych i zadań pomocniczych.

Wyświetlanie pobranych uaktualnień

W celu wyświetlenia listy pobranych uaktualnień:

W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Aktualizacje baz danych i modułów oprogramowania Kaspersky**.

Obszar roboczy folderu **Aktualizacje baz danych i modułów oprogramowania Kaspersky** wyświetla listę aktualizacji zapisanych na Serwerze administracyjnym.

Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach

Możesz skonfigurować automatyczne aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security na urządzeniach klienckich.

W celu skonfigurowania pobierania i automatycznej instalacji uaktualnień dla Kaspersky Endpoint Security na urządzeniach:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Utwórz zadanie **Aktualizacja** w jeden z następujących sposobów:
   - Wybierając **Nowe** → **Zadanie** w menu kontekstowym folderu **Zadania** w drzewie konsoli.
   - Kliknij przycisk **Nowe zadanie** dostępny w obszarze roboczym folderu **Zadania**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. W oknie **Wybierz typ zadania** kreatora, jako typ zadania wybierz **Kaspersky Endpoint Security**, a następnie, jako podtyp zadania wskaż **Aktualizacja**.
4. Wykonaj pozostałe instrukcje kreatora.

   Po zakończeniu pracy kreatora zostanie utworzone zadanie aktualizacji dla Kaspersky Endpoint Security. Nowo utworzone zadanie będzie wyświetlane na liście zadań, w obszarze roboczym folderu **Zadania**.
5. W obszarze roboczym folderu **Zadania** wybierz utworzone zadanie aktualizacji.
6. Z menu kontekstowego zadania wybierz **Właściwości**.
7. W otwartym oknie właściwości zadania, w panelu **Sekcje** wybierz **Opcje**.

   W sekcji **Opcje** możesz zdefiniować ustawienia zadania aktualizacji w trybie lokalnym lub mobilnym:
   - **Ustawienia aktualizacji dla trybu lokalnego**: Połączenie jest nawiązywane między urządzeniem a Serwerem administracyjnym.
   - **Ustawienia aktualizacji dla trybu mobilnego**: Połączenie pomiędzy Kaspersky Security Center a urządzeniem nie jest nawiązywane (na przykład, jeśli urządzenie nie jest podłączone do internetu).
8. Kliknij przycisk **Ustawienia**, aby wybrać źródło uaktualnień.
9. Wybierz opcję **Pobierz uaktualnienia modułów aplikacji**, aby pobrać i zainstalować uaktualnienia modułów aplikacji wraz z bazami danych aplikacji.

   Jeśli pole jest zaznaczone, Kaspersky Endpoint Security powiadamia użytkownika o dostępnych uaktualnieniach modułów aplikacji i włącza uaktualnienia modułów aplikacji do pakietu aktualizacyjnego podczas wykonywania zadania aktualizacji. Skonfiguruj użycie modułów aktualizacji:

- **Zainstaluj krytyczne i zatwierdzone aktualizacje**. Jeśli dla modułów aplikacji dostępne są jakiekolwiek aktualizacje, Kaspersky Endpoint Security automatycznie zainstaluje te ze stanem *Krytyczne*. Pozostałe aktualizacje zostaną zainstalowane, jak je zatwierdzisz.

- **Zainstaluj tylko zatwierdzone aktualizacje**. Jeśli dla modułów aplikacji dostępne są jakiekolwiek aktualizacje, Kaspersky Endpoint Security zainstaluje je po zatwierdzeniu ich instalacji. Zostaną one zainstalowane lokalnie, poprzez interfejs aplikacji lub poprzez Kaspersky Security Center.

Jeśli do zainstalowania uaktualnień modułów aplikacji wymagane jest przejrzenie i zaakceptowanie warunków Umowy licencyjnej i Polityki prywatności, aplikacja zainstaluje uaktualnienia po zaakceptowaniu warunków Umowy licencyjnej i Polityki prywatności przez użytkownika.

10. Wybierz opcję **Kopiuj uaktualnienia do folderu**, aby aplikacja zapisywała pobrane uaktualnienia w folderze, a następnie kliknij przycisk **Przeglądaj**, aby określić folder.

11. Kliknij **OK**.

Podczas wykonywania zadania **Aktualizacja** aplikacja wysyła żądanie do serwerów aktualizacji Kaspersky.

Niektóre aktualizacje wymagają zainstalowania najnowszych wersji wtyczek zarządzających.

Tryb offline pobierania uaktualnień

Agent sieciowy na zarządzanych urządzeniach może czasami nie nawiązać połączenia z Serwerem administracyjnym w celu pobrania uaktualnień. Na przykład Agent sieciowy mógł zostać zainstalowany na laptopie, który czasami nie ma połączenia z internetem oraz nie ma dostępu do sieci lokalnej. Co więcej, administrator mógł ograniczyć czas połączenia urządzeń z siecią. W takich przypadkach, urządzenia z zainstalowanym Agentem sieciowym nie mogą pobierać uaktualnień z Serwera administracyjnego zgodnie z istniejącym terminarzem. Jeśli skonfigurowałeś aktualizację zarządzanych aplikacji (na przykład Kaspersky Endpoint Security) przy użyciu Agenta sieciowego, każda aktualizacja będzie wymagała połączenia z Serwerem administracyjnym. Jeśli połączenie między Agentem sieciowym a Serwerem administracyjnym nie zostanie nawiązane, aktualizacja nie będzie mogła zostać przeprowadzona. Możesz skonfigurować połączenie między Agentem sieciowym a Serwerem administracyjnym tak, aby Agent sieciowy łączył się z Serwerem administracyjnych w określonych przedziałach czasu. W najgorszym razie, jeśli określone odstępy między połączeniami pokrywają się z przedziałami czasu, gdy połączenie jest dostępne, bazy danych nigdy nie zostaną zaktualizowane. Dodatkowo, gdy kilka zarządzanych aplikacji jednocześnie spróbuje uzyskać dostęp do Serwera administracyjnego w celu pobrania uaktualnień, mogą pojawić się problemy. W tej sytuacji, Serwer administracyjny może przestać odpowiadać na żądania (podobnie, jak w przypadku ataku DDoS).

Aby uniknąć wyżej opisanych problemów, w Kaspersky Security Center zaimplementowano tryb offline do pobierania uaktualnień i modułów zarządzanych aplikacji. Ten tryb oferuje mechanizm dystrybucji uaktualnień, niezależnie od tymczasowych problemów spowodowanych przez brak dostępności kanałów komunikacyjnych Serwera administracyjnego. Ten model zmniejsza także obciążenie na Serwerze administracyjnym.

Działanie trybu offline pobierania uaktualnień

Jeśli Serwer administracyjny pobierze uaktualnienia, powiadomi Agenta sieciowego (na urządzeniach, na których jest zainstalowany) o uaktualnieniach, które będą wymagane dla zarządzanych aplikacji. Jeśli Agent sieciowy otrzyma informacje o tych uaktualnieniach, pobierze odpowiednie pliki z Serwera administracyjnego z wyprzedzeniem. Przy pierwszym nawiązaniu połączenia z Agentem sieciowym, Serwer administracyjny inicjuje pobranie uaktualnień. Jeśli Agent sieciowy pobierze wszystkie uaktualnienia na urządzenie klienckie, staną się one dostępne dla aplikacji na tym urządzeniu.

Jeśli zarządzana aplikacja na urządzeniu klienckim spróbuje uzyskać dostęp do Agenta sieciowego w celu uzyskania uaktualnień, Agent sieciowy sprawdzi, czy posiada wszystkie wymagane uaktualnienia. Jeśli uaktualnienia zostały pobrane z Serwera administracyjnego nie więcej niż 25 godzin przed zażądaniem ich przez zarządzaną aplikację, Agent sieciowy nie nawiąże połączenia z Serwerem administracyjnym, ale dostarczy zarządzanej aplikacji uaktualnienia z lokalnej pamięci podręcznej. Połączenie z Serwerem administracyjnym może nie zostać nawiązane, gdy Agent sieciowy dostarcza uaktualnienia aplikacji na urządzeniach klienckich, ale połączenie nie jest wymagane w celu przeprowadzenia aktualizacji.

Aby równomiernie rozłożyć obciążenie Serwera administracyjnego, Agent sieciowy na urządzeniu nawiązuje połączenie z Serwerem administracyjnym i pobiera uaktualnienia w kolejności losowej w obrębie przedziału czasu określonego przez Serwer administracyjny. Długość tego przedziału czasu zależy od liczby urządzeń z zainstalowanym Agentem sieciowym, który pobiera uaktualnienia, oraz od rozmiaru tych uaktualnień. Aby zmniejszyć obciążenie na Serwerze administracyjnym, jako punkty dystrybucji można użyć Agenty sieciowe.

Jeśli tryb offline pobierania uaktualnień jest wyłączony, uaktualnienia są rozsyłane zgodnie z terminarzem zadania pobierania uaktualnień.

Domyślnie włączony jest tryb offline pobierania uaktualnień.

Tryb offline do pobierania uaktualnień jest używany tylko na zarządzanych urządzeniach, na których dla zadania pobierania uaktualnień przez zarządzane aplikacje jako typ terminarza wybrano **Po pobraniu nowych uaktualnień do repozytorium**. Dla innych zarządzanych urządzeń wykorzystywany jest standardowy schemat pobierania uaktualnień z Serwera administracyjnego w czasie rzeczywistym.

Zalecane jest wyłączenie trybu offline do pobierania uaktualnień przy użyciu ustawień profili Agenta sieciowego odpowiednich grup administracyjnych w następujących przypadkach: jeśli dla zarządzanych aplikacji pobieranie uaktualnień nie zostało ustawione z Serwera administracyjnego, ale z serwerów Kaspersky lub z folderu sieciowego, a dla zadania pobierania uaktualnień wybrano typ terminarza **Po pobraniu nowych uaktualnień do repozytorium**.

Włączanie i wyłączanie trybu offline pobierania uaktualnień

Nie jest zalecane wyłączanie trybu offline pobierania uaktualnień. Wyłączenie tego trybu może spowodować błędy w dostarczeniu uaktualnień na urządzenia. W niektórych przypadkach specjalista z pomocy technicznej Kaspersky może zalecić odznaczenie pola **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem**. Następnie upewnij się, że zadanie pobierania uaktualnień dla aplikacji firmy Kaspersky zostało skonfigurowane.

W celu włączenia lub wyłączenia trybu offline pobierania uaktualnień dla grupy administracyjnej:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz włączyć tryb offline pobierania uaktualnień.
2. W obszarze roboczym grupy otwórz zakładkę **Zasady**.
3. Na zakładce **Zasady** wybierz profil Agenta sieciowego.
4. Z otwartego menu kontekstowego zasady wybierz **Właściwości**.

   Otwórz okno właściwości profilu Agenta sieciowego.

5. W oknie właściwości zasady wybierz sekcję **Zarządzaj poprawkami i aktualizacjami**.

6. Zaznacz lub odznacz pole **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)**, aby włączyć lub wyłączyć model offline pobierania uaktualnień.

   Domyślnie włączony jest tryb offline pobierania uaktualnień.

Tryb offline pobierania uaktualnień zostanie włączony lub wyłączony.

Automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center

Domyślnie, wszelkie pobrane uaktualnienia i poprawki są instalowane automatycznie dla następujących komponentów:

- Agent sieciowy dla systemu Windows
- Konsola administracyjna
- Serwer urządzeń mobilnych Exchange
- Serwer iOS MDM

Automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center jest dostępne tylko dla urządzeń działających pod kontrolą systemu Windows. Możesz wyłączyć automatyczne aktualizowanie i instalowanie poprawek dla tych komponentów. W tym przypadku wszelkie pobrane uaktualnienia i poprawki zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzono*. Uaktualnienia i łaty ze stanem *Nie zdefiniowano* nie zostaną zainstalowane.

Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center

Automatyczna instalacja uaktualnień i łat dla komponentów Kaspersky Security Center jest włączona domyślnie podczas instalacji Agenta sieciowego na urządzeniu. Możesz to wyłączyć podczas instalacji Agenta sieciowego lub wyłączyć później przy użyciu profilu.

W celu wyłączenia automatycznej aktualizacji i instalacji poprawek dla komponentów Kaspersky Security Center podczas lokalnej instalacji Agenta sieciowego na urządzeniu:

1. Uruchom lokalną instalację Agenta sieciowego na urządzeniu.

2. W kroku **Ustawienia zaawansowane** odznacz pole **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**.

3. Postępuj zgodnie z instrukcjami kreatora.

Na urządzeniu zostanie zainstalowany Agent sieciowy z wyłączoną automatyczną aktualizacją i instalacją łat dla komponentów Kaspersky Security Center. Automatyczne aktualizowanie i instalowanie poprawek można włączyć w późniejszym czasie, korzystając z profilu.

W celu wyłączenia automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center podczas instalacji Agenta sieciowego na urządzeniu przy użyciu pakietu instalacyjnego:

1. Z drzewa konsoli wybierz folder **Zdalna instalacja** → **Pakiety instalacyjne**.
2. W menu kontekstowym pakietu **Agent sieciowy Kaspersky Security Center <numer wersji>** wybierz **Właściwości**.
3. We właściwościach pakietu instalacyjnego, w sekcji **Ustawienia** odznacz pole **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**.

Z tego pakietu zostanie zainstalowany Agent sieciowy z wyłączoną automatyczną aktualizacją i instalacją łat dla komponentów Kaspersky Security Center. Automatyczne aktualizowanie i instalowanie poprawek można włączyć w późniejszym czasie, korzystając z profilu.

Jeśli to pole zostało zaznaczone (lub odznaczone) podczas instalacji Agenta sieciowego na urządzeniu, możesz włączyć (lub wyłączyć) automatyczne aktualizowanie przy użyciu profilu Agenta sieciowa.

W celu włączenia lub wyłączenia automatycznego aktualizowania i instalowania poprawek dla składników Kaspersky Security Center przy użyciu profilu Agenta sieciowego:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz włączyć lub wyłączyć automatyczne aktualizowanie i instalowanie poprawek.
2. W obszarze roboczym grupy otwórz zakładkę **Zasady**.
3. Na zakładce **Zasady** wybierz profil Agenta sieciowego.
4. Z otwartego menu kontekstowego zasady wybierz **Właściwości**.

   Otwórz okno właściwości profilu Agenta sieciowego.
5. W oknie właściwości zasady wybierz sekcję **Zarządzaj poprawkami i aktualizacjami**.
6. Zaznacz lub odznacz pole **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**, aby włączyć lub wyłączyć automatyczne aktualizowanie i instalowanie poprawek.
7. Ustaw blokadę dla tego pola.

Profil zostanie zastosowany na wybranych urządzeniach, a automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center zostanie włączone (lub wyłączone) na tych urządzeniach.

Automatyczne rozsyłanie uaktualnień

Kaspersky Security Center pozwala na automatyczne rozsyłanie i instalację uaktualnień na urządzeniach klienckich i podrzędnych Serwerach administracyjnych.

Automatyczne rozsyłanie uaktualnień do urządzeń klienckich

W celu automatycznego rozesłania uaktualnień wybranych aplikacji do urządzeń klienckich natychmiast po ich pobraniu do repozytorium Serwera administracyjnego:

1. Nawiąż połączenie z Serwerem administracyjnym, który zarządza urządzeniami klienckimi.
2. Utwórz zadanie zdalnej instalacji uaktualnień dla wybranych urządzeń klienckich w jeden z następujących sposobów:
   - Jeśli chcesz rozesłać uaktualnienia do urządzeń klienckich należących do wybranej grupy administracyjnej, utwórz zadanie dla wybranej grupy.
   - Jeżeli chcesz rozesłać uaktualnienia do urządzeń klienckich należących do różnych grup administracyjnych lub nie będących w żadnej grupie administracyjnej, utwórz zadanie dla wskazanych urządzeń.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z jego instrukcjami i wykonaj następujące czynności:

   a. W oknie **Typ zadania**, w węźle żądanej aplikacji wybierz zadanie rozsyłania uaktualnień.

      Nazwa zadania rozsyłania uaktualnień wyświetlana w oknie **Typ zadania** zależy od aplikacji, dla której utworzyłeś to zadanie. Szczegółowe informacje o nazwach zadań aktualizacji dla wybranych aplikacji Kaspersky znajdziesz w odpowiedniej dokumentacji.

   b. W oknie kreatora **Terminarz**, w polu **Zaplanowane uruchomienie** wybierz **Po pobraniu nowych uaktualnień do repozytorium**.

   Nowo utworzone zadanie rozsyłania uaktualnień będzie uruchamiane dla wybranych urządzeń za każdym razem po pobraniu uaktualnień do repozytorium Serwera administracyjnego.

Jeśli zadanie rozsyłania uaktualnień dla wybranej aplikacji zostało utworzone dla wybranych urządzeń, aby automatycznie rozesłać uaktualnienia na urządzenia klienckie, w oknie właściwości zadania, w sekcji **Terminarz** wybierz opcję **Po pobraniu nowych uaktualnień do repozytorium** w polu **Zaplanowane uruchomienie**.

Automatyczne rozsyłanie uaktualnień do podrzędnych Serwerów administracyjnych

W celu rozesłania uaktualnień wybranych aplikacji do podrzędnych Serwerów administracyjnych natychmiast po ich pobraniu do repozytorium nadrzędnego Serwera administracyjnego:

1. W drzewie konsoli, w węźle głównego Serwera administracyjnego wybierz folder **Zadania**.
2. Na liście zadań w obszarze roboczym wybierz zadanie Serwera administracyjnego: Pobierz uaktualnienia do repozytorium Serwera administracyjnego.
3. Otwórz sekcję **Ustawienia** wybranego zadania w jeden z następujących sposobów:
   - Wybierając **Właściwości** w menu kontekstowym zadania.
   - Klikając odnośnik **Modyfikuj ustawienia** w oknie z informacjami dla wybranego zadania.
4. W sekcji **Ustawienia**, dostępnej w oknie właściwości zadania, przejdź do podsekcji **Inne ustawienia** i kliknij odnośnik **Konfiguruj**.
5. W otwartym oknie **Inne ustawienia** zaznacz pole **Wymuś aktualizację podrzędnych Serwerów administracyjnych**.

W oknie ustawień zadania pobierania uaktualnień Serwera administracyjnego, na zakładce **Ustawienia** zaznacz pole **Wymuś aktualizację podrzędnych Serwerów administracyjnych**.

Po pobraniu uaktualnień przez główny Serwer administracyjny, zadania pobierania uaktualnień zostaną automatycznie uruchomione na podrzędnych Serwerach administracyjnych bez względu na ich terminarz.

Automatyczne przypisywanie punktów dystrybucji

Zalecane jest automatyczne przypisywanie punktów dystrybucji. Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji.

Aby automatycznie przypisać punkty dystrybucji:

1. Otwórz okno główne aplikacji.
2. W drzewie konsoli należy wybrać węzeł z nazwą Serwera administracyjnego, dla którego chcesz automatycznie przypisać punkty dystrybucji.
3. W menu kontekstowym Serwera administracyjnego kliknij **Właściwości**.
4. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Punkty dystrybucji**.
5. W prawej części okna wybierz opcję **Automatycznie przypisz punkty dystrybucji**.

   Jeśli włączone jest automatyczne wskazywanie urządzeń jako punktów dystrybucji, nie można ręcznie skonfigurować punktów dystrybucji, ani też zmodyfikować listy punktów dystrybucji.

6. Kliknij **OK**.

Serwer administracyjny automatycznie przypisze i skonfiguruje punkty dystrybucji.

Ręczne wskazywanie urządzenia jako punktu dystrybucji

Kaspersky Security Center umożliwia wskazanie urządzeń do pełnienia roli punktów dystrybucji.

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji. Jednakże, jeśli z jakiegoś powodu musisz zrezygnować z automatycznego przypisywania punktów dystrybucji (na przykład, jeśli chcesz korzystać ze specjalnie wybranych serwerów), możesz ręcznie przypisać punkty dystrybucji po obliczeniu ich liczby i konfiguracji.

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

W celu ręcznego wskazania urządzenia jako punktu dystrybucji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji** i kliknij przycisk **Dodaj**. Ten przycisk jest dostępny, jeśli zaznaczono opcję **Ręcznie przypisz punkty dystrybucji**.

   Spowoduje to otwarcie okna **Dodaj punkt dystrybucji**.

4. W oknie **Dodaj punkt dystrybucji** wykonaj następujące działania:

   a. Wybierz urządzenie, które będzie pełniło rolę punktu dystrybucji (wybierz je z grupy administracyjnej lub określ adres IP urządzenia). Podczas wybierania urządzenia pamiętaj o zasadach działania punktów dystrybucji i wymaganiach ustawionych dla urządzenia pełniącego rolę punktu dystrybucji.

   b. Wskaż określone urządzenia, na które punkt dystrybucji roześle uaktualnienia. Możesz określić opis grupy administracyjnej lub lokalizacji sieciowej.

5. Kliknij **OK**.

   Dodany punkt dystrybucji będzie wyświetlany na liście punktów dystrybucji, w sekcji **Punkty dystrybucji**.

6. Na liście wskaż nowo dodany punkt dystrybucji i kliknij przycisk **Właściwości**, aby otworzyć jego okno właściwości.

7. Skonfiguruj punkt dystrybucji w oknie właściwości:

   - Sekcja **Ogólny** zawiera ustawienia interakcji pomiędzy punktem dystrybucji a urządzeniami klienckimi.

     - **Port SSL**

       Numer portu SSL do nawiązywania zaszyfrowanych połączeń między urządzeniami klienckimi a punktem dystrybucji przy użyciu SSL.

       Domyślnie wykorzystywany jest port 13000.

     - **Użyj multiemisji**

       Jeśli ta opcja jest włączona, multicasting IP będzie używany do automatycznego rozsyłania pakietów instalacyjnych na urządzenia klienckie w obrębie grupy.

       Multiemisja IP zmniejsza czas wymagany do zainstalowania aplikacji z pakietu instalacyjnego w grupie urządzeń klienckich, ale zwiększa czas instalacji, gdy instalujesz aplikację na jednym urządzeniu klienckim.

     - **Adres IP multiemisji**

       Adres IP, który będzie używany do multiemisji. Możesz zdefiniować adres IP z zakresu 224.0.0.0 – 239.255.255.255

       Domyślnie, Kaspersky Security Center automatycznie przypisze unikatowy adres IP multiemisji w obrębie danego zakresu.

     - **Numer portu multiemisji IP**

       Numer portu do multiemisji IP.

       Domyślnym numerem portu jest 15001. Jeśli jako punkt dystrybucji określono urządzenie, na którym działa Serwer administracyjny, domyślnie dla połączenia SSL używany jest port 13001.

     - **Roześlij aktualizacje**

Aktualizacje są dystrybuowane na zarządzane urządzenia z następujących źródeł:

- Ten punkt dystrybucji, jeśli ta opcja jest włączona.
- Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

Jeśli używasz punktów dystrybucji do wdrażania aktualizacji, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

Jeśli wyłączysz tę opcję, liczba pobrań aktualizacji i obciążenia Serwera administracyjnego mogą wzrosnąć. Domyślnie opcja ta jest włączona.

- **Roześlij pakiety instalacyjne**

  Pakiety instalacyjne są dystrybuowane na zarządzane urządzenia z następujących źródeł:

  - Ten punkt dystrybucji, jeśli ta opcja jest włączona.
  - Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

  Jeśli używasz punktów dystrybucji do wdrażania pakietów instalacyjnych, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

  Jeśli wyłączysz tę opcję, liczba pobrań pakietów instalacyjnych i obciążenie Serwera administracyjnego może wzrosnąć. Domyślnie opcja ta jest włączona.

- **Użyj tego punktu dystrybucji jako serwera push**

  W Kaspersky Security Center punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

  Jeśli zarządzasz urządzeniami z zainstalowanym KasperskyOS lub planujesz to zrobić, musisz użyć punktu dystrybucji jako serwera push. Możesz także użyć punktu dystrybucji jako serwera push, jeśli chcesz wysłać powiadomienia push na urządzenia klienckie.

- **Port serwera push**

  Port na punkcie dystrybucji, którego urządzenia klienckie użyją do nawiązania połączenia. Domyślnie wykorzystywany jest port 13295.

- W sekcji **Zakres** określ obszar, w jakim punkt dystrybucji będzie rozsyłał uaktualnienia (grupy administracyjne i/lub lokalizacja sieciowa).
- W sekcji **KSN Proxy** możesz skonfigurować aplikację, aby używała punktu dystrybucji do przesyłania żądań KSN z zarządzanych urządzeń.

- **Włącz KSN Proxy po stronie punktu dystrybucji**

  Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

  Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky. Domyślnie, Oświadczenie KSN znajduje się w %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

  Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

- **Przesyłaj żądania KSN do Serwera administracyjnego**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dostęp do chmury KSN / Private KSN bezpośrednio przez internet**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub Private KSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub Private KSN.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej), nie może uzyskać bezpośredniego dostępu do Private KSN. Jeśli chcesz ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do prywatnej sieci KSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 12 (lub późniejszej), może uzyskać bezpośredni dostęp do Private KSN.

- **Ignoruj ustawienia serwera proxy w przypadku łączenia z Private KSN**

  Włącz tę opcję, jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach punktu dystrybucji lub w zasadzie Agenta sieciowego, ale architektura Twojej sieci wymaga bezpośredniego korzystania z Private KSN. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do Private KSN.

  Ta opcja jest dostępna, jeśli wybierzesz opcję **Dostęp do KSN Cloud/Private KSN bezpośrednio przez Internet**.

- **Port TCP**

  Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

- **Port UDP**

  Jeśli chcesz, żeby zarządzane urządzenia nawiązywały połączenie z serwerem KSN proxy poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

- W sekcji **Wykrywanie urządzeń** skonfiguruj przeszukiwanie domen Windows, Active Directory i zakresów IP przez punkt dystrybucji.

  - **Domeny Windows**

    Możesz włączyć wykrywanie urządzeń dla domen Windows i ustawić terminarz dla wyszukiwania.

  - **Active Directory**

    Możesz włączyć przeszukiwanie sieci dla Active Directory i ustawić terminarz dla przeszukiwania.

    Jeśli zaznaczysz pole **Enable Active Directory polling**, możesz wybrać jedną z następujących opcji:

    - **Przeszukaj bieżącą domenę Active Directory**.
    - **Przeszukaj las domen Active Directory**.
    - **Przeszukaj tylko wybrane domeny Active Directory**. Jeśli wybierzesz tę opcję, dodaj jedną lub kilka domen Active Directory do listy.

  - **Zakresy IP**

    Możesz włączyć wykrywanie urządzeń dla zakresów IPv4 i sieci IPv6.

    Jeśli włączysz opcję **Włącz przeszukiwanie zakresów**, możesz dodać skanowane zakresy i skonfigurować dla nich terminarz. Możesz dodać zakresy IP do listy skanowanych zakresów.

    Jeśli włączysz opcję **Użyj Zeroconf do przeszukiwania sieci IPv6**, punkt dystrybucji automatycznie odpytuje sieć IPv6 za pomocą zero-configuration networking (zwany również *Zeroconf*). W takim przypadku określone zakresy adresów IP są ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć. Opcja **Użyj Zeroconf do przeszukiwania sieci IPv6** jest dostępna, jeśli w punkcie dystrybucji działa system Linux. Aby korzystać z odpytywania Zerocong IPv6, musisz zainstalować narzędzie avahi-browse w punkcie dystrybucji.

- W sekcji **Zaawansowane** określ folder, którego punkt dystrybucji musi używać do przechowywania rozsyłanych danych.

  - **Użyj domyślnego folderu**

    Jeśli wybierzesz tę opcję, aplikacja użyje folderu instalacyjnego Agenta sieciowego na urządzeniu działającym jako punkt dystrybucji.

  - **Użyj określonego folderu**

    Jeśli wybierzesz tę opcję, w polu poniżej możesz określić ścieżkę dostępu do wybranego folderu. Może to być folder lokalny na urządzeniu działającym jako punkt dystrybucji lub folder na dowolnym urządzeniu w obrębie sieci korporacyjnej.

    Konto użytkownika używane na urządzeniu działającym jako punkt dystrybucji do uruchamiania Agenta sieciowego musi mieć uprawnienia do odczytu/zapisu określonego folderu.

Wybrane urządzenia będą pełnić rolę punktów dystrybucji.

Tylko urządzenia działające pod kontrolą systemu operacyjnego Windows mogą determinować swoją lokalizację sieciową. Lokalizacja sieciowa nie może zostać określona dla urządzeń z zainstalowanymi innymi systemami operacyjnymi.

Usuwanie urządzenia z listy punktów dystrybucji

W celu usunięcia urządzenia z listy punktów dystrybucji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **Punkty dystrybucji** wybierz urządzenie, które pełni rolę punktu dystrybucji, i kliknij przycisk **Usuń**.

Urządzenie zostanie usunięte z listy punktów dystrybucji i przestanie działać jako punkt dystrybucji.

Urządzenia nie można usunąć z listy punktów dystrybucji, jeśli zostało przypisane automatycznie przez Serwer administracyjny.

Pobieranie uaktualnień przez punkty dystrybucji

Kaspersky Security Center umożliwia punktom dystrybucji pobieranie uaktualnień z Serwera administracyjnego, serwerów Kaspersky bądź też folderu lokalnego lub sieciowego.

W celu skonfigurowania pobierania uaktualnień dla punktu dystrybucji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **Punkty dystrybucji** wybierz punkt dystrybucji, przez którego uaktualnienia będą dostarczane na urządzenia klienckie w grupie.
4. Kliknij przycisk **Właściwości**, aby otworzyć okno właściwości wybranego punktu dystrybucji.
5. W oknie właściwości punktu dystrybucji wybierz sekcję **Źródła aktualizacji**.
6. Wskaż źródło uaktualnień dla punktu dystrybucji:
   - Aby zezwolić punktowi dystrybucji na pobieranie uaktualnień z Serwera administracyjnego, zaznacz opcję **Pobierz z Serwera administracyjnego**:
     - Pobierz pliki diff

Ta opcja włącza funkcję pobierania plików diff.

Domyślnie opcja ta jest włączona.

- Aby zezwolić punktowi dystrybucji na pobieranie uaktualnień przy użyciu zadania, wybierz **Użyj zadania do wymuszonego pobierania uaktualnień**:
  - Kliknij przycisk **Przeglądaj**, jeśli takie zadanie już istnieje na urządzeniu, i wybierz zadanie z listy, która zostanie wyświetlona.
  - Kliknij przycisk **Nowe zadanie**, aby utworzyć zadanie, jeśli nie ma go na urządzeniu. Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

Zadanie Pobierz uaktualnienia do repozytoriów punktów dystrybucji to zadanie lokalne. Należy utworzyć nowe zadanie dla każdego urządzenia pełniącego rolę punktu dystrybucji.

Punkt dystrybucji będzie pobierał uaktualnienia z określonego źródła.

Usuwanie aktualizacji oprogramowania z repozytorium

W celu usunięcia aktualizacji oprogramowania z repozytorium Serwera administracyjnego:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.
2. W obszarze roboczym folderu **Aktualizacje oprogramowania** wybierz uaktualnienie, które chcesz usunąć.
3. W menu kontekstowym uaktualnienia wybierz **Usuń pliki aktualizacji**.

Aktualizacje oprogramowania zostaną usunięte z repozytorium Serwera administracyjnego.

Instalacja poprawki dla aplikacji Kaspersky w trybie klastra

Kaspersky Security Center obsługuje tylko ręczną instalacje łat dla aplikacji Kaspersky w trybie klastra.

W celu zainstalowania łaty dla aplikacji Kaspersky:

1. Pobierz łatę do każdego węzła klastra.
2. Uruchom instalację łaty na aktywnym węźle.
3. Poczekaj na pomyślne zainstalowanie łaty.
4. Uruchom łatę na wszystkich podwęzłach klastra po kolei.

   Jeśli uruchamiasz łatę z poziomu wiersza poleceń, użyj przełącznika `-CLUSTER_SECONDARY_NODE`.

   Łata zostanie zainstalowana na wszystkich węzłach klastra.

5. Uruchom usługi klastra Kaspersky ręcznie.

Każdy węzeł klastra jest wyświetlany w Konsoli administracyjnej jako urządzenie z zainstalowanym Agentem sieciowym.

Informacje na temat zainstalowanych łat można znaleźć w folderze **Aktualizacje oprogramowania** lub w raporcie o wersjach aktualizacji modułów aplikacji Kaspersky.

Zarządzanie aplikacjami firm trzecich na urządzeniach klienckich

Kaspersky Security Center umożliwia zarządzanie aplikacjami firmy Kaspersky i innych producentów, które są zainstalowane na urządzeniach klienckich.

Administrator może wykonywać następujące akcje:

- Tworzyć kategorie aplikacji w oparciu o określone kryteria.
- Zarządzać kategoriami aplikacji przy pomocy reguł utworzonych specjalnie do tego celu.
- Zarządzać aplikacjami uruchomionymi na urządzeniach.
- Przeprowadzać inwentaryzację i utrzymywać rejestr oprogramowania zainstalowanego na urządzeniach.
- Naprawiać luki w oprogramowaniu zainstalowanym na urządzeniach.
- Instalować uaktualnienia z Windows Update i od producentów innego oprogramowania na urządzeniach.
- Monitorować korzystanie z kluczy licencyjnych dla grup licencjonowanych aplikacji.

Instalowanie aktualizacji oprogramowania firm trzecich

Kaspersky Security Center umożliwia zarządzanie aktualizacjami oprogramowania zainstalowanego na urządzeniach klienckich oraz wyeliminowanie luk w aplikacjach Microsoft i produktach innych dostawców poprzez zainstalowanie żądanych aktualizacji.

Kaspersky Security Center wyszukuje aktualizacje przy pomocy zadania wyszukiwania aktualizacji i pobiera je do repozytorium uaktualnień. Po zakończeniu wyszukiwania aktualizacji, aplikacja udostępnia administratorowi informacje o dostępnych aktualizacjach i lukach w aplikacji, które mogą zostać naprawione dzięki tym aktualizacjom.

Informacje o aktualizacjach dostępnych dla Microsoft Windows są dostępne poprzez usługę Windows Update. Serwer administracyjny może zostać użyty jako serwer Windows Server Update Services (WSUS). Aby używać Serwera administracyjnego jako serwera WSUS, powinieneś skonfigurować synchronizację aktualizacji z Windows Update. Po skonfigurowaniu synchronizacji danych z Windows Update, Serwer administracyjny zapewnia aktualizacje dla usług Windows Update na urządzeniach w trybie scentralizowanym i z określoną częstotliwością.

Możesz również zarządzać aktualizacjami oprogramowania poprzez profil Agenta sieciowego. W tym celu, w odpowiednich oknach kreatora tworzenia nowego profilu powinieneś utworzyć profil Agenta sieciowego i skonfigurować aktualizowanie oprogramowania.

Administrator może przeglądać listę dostępnych aktualizacji w podfolderze **Aktualizacje oprogramowania** znajdującym się w folderze **Zarządzanie aplikacjami**. Ten folder zawiera listę uaktualnień pobranych przez Serwer administracyjny dla aplikacji Microsoft i innych producentów oprogramowania, które mogą być przesyłane na urządzenia. Po przejrzeniu informacji o dostępnych aktualizacjach, administrator może zainstalować je na urządzeniach.

Kaspersky Security Center aktualizuje niektóre aplikacje poprzez usunięcie poprzedniej wersji aplikacji i instalację nowej.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu złośliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk w zabezpieczeniach (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Przed zainstalowaniem uaktualnień na wszystkich urządzeniach możesz przeprowadzić instalację testową, aby upewnić się, że zainstalowane uaktualnienia nie spowodują błędu w działaniu aplikacji na urządzeniach.

Szczegółowe informacje dotyczące oprogramowania firm trzecich, które może być aktualizowane poprzez Kaspersky Security Center, można znaleźć na stronie działu pomocy technicznej, na podstronie poświęconej Kaspersky Security Center, w sekcji Zarządzanie serwerem.

Scenariusz: Aktualizowanie oprogramowania innej firmy

Ta sekcja oferuje scenariusz aktualizacji oprogramowania innej firmy, zainstalowanego na urządzeniach klienckich. Oprogramowanie firm trzecich obejmuje aplikacje firmy Microsoft oraz programy innych firm. Aktualizacje dla aplikacji firmy Microsoft są dostarczane przez usługę Windows Update.

Wymagania wstępne

Serwer administracyjny musi mieć połączenie z Internetem, aby zainstalować aktualizacje oprogramowania firm trzecich innego niż oprogramowanie firmy Microsoft.

Domyślnie połączenie internetowe w przypadku Serwera administracyjnego nie jest wymagane w celu instalowania aktualizacji oprogramowania firmy Microsoft na zarządzanych urządzeniach. Na przykład zarządzane urządzenia mogą pobierać aktualizacje oprogramowania firmy Microsoft bezpośrednio z serwerów Microsoft Update lub z systemu Windows Server z programem Microsoft Windows Server Update Services (WSUS) wdrożonymi w sieci organizacji. Serwer administracyjny musi być połączony z Internetem, jeśli jest on używany jako serwer WSUS.

Etapy

Aktualizowanie oprogramowania firm trzecich odbywa się w etapach:

1. **Wyszukiwanie wymaganych aktualizacji**

   Aby odnaleźć aktualizacje oprogramowania firm trzecich dla zarządzanych urządzeń, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

   Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Serwera administracyjnego. Jeśli nie uruchomiono kreatora, utwórz zadanie lub uruchom Kreator wstępnej konfiguracji teraz.

   Dostępne instrukcje:

   - Konsola administracyjna: Skanowanie aplikacji w poszukiwaniu luk, Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console: Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji, Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

2. **Analizowanie listy wykrytych aktualizacji**

   Przejrzyj listę **Aktualizacje oprogramowania** i zdecyduj, które aktualizacje chcesz zainstalować. Aby przejrzeć szczegółowe informacje o każdej aktualizacji, kliknij nazwę aktualizacji na liście. Dla każdej aktualizacji na liście możesz także przejrzeć statystyki dotyczące instalacji aktualizacji na urządzeniach klienckich.

   Dostępne instrukcje:

   - Konsola administracyjna: Przeglądanie informacji o dostępnych aktualizacjach
   - Kaspersky Security Center Web Console: Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

3. **Konfigurowanie instalacji aktualizacji**

   Jeśli Kaspersky Security Center odebrał listę aktualizacji oprogramowania firm trzecich, możesz zainstalować je na urządzeniach klienckich przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki* lub zadania *Zainstaluj aktualizacje Windows Update*. Utwórz jedno z tych zadań. Możesz utworzyć te zadania na zakładce **Zadania** lub korzystając z listy **Aktualizacje oprogramowania**.

   Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do zainstalowania aktualizacji dla aplikacji firmy Microsoft, w tym aktualizacji dostarczonych przez usługę Windows Update, a także aktualizacji produktów innych producentów. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami.

   Zadanie *Zainstaluj aktualizacje Windows Update* nie wymaga licencji, ale może zostać użyte tylko do zainstalowania aktualizacji Windows Update.

   Aby zainstalować niektóre aktualizacje oprogramowania, należy zaakceptować Umowę licencyjną do zainstalowania oprogramowania. Jeśli odrzucisz Umowę licencyjną, aktualizacja oprogramowania nie zostanie zainstalowana.

   Możesz uruchomić zadanie instalacji aktualizacji zgodnie z terminarzem. Podczas określania terminarza zadania upewnij się, że zadanie instalacji aktualizacji jest uruchamiane po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

   Dostępne instrukcje:

   - Konsola administracyjna: Naprawianie luk w aplikacjach, Przeglądanie informacji o dostępnych aktualizacjach
   - Kaspersky Security Center Web Console: Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki, Tworzenie zadania Zainstaluj aktualizacje Windows Update, Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

4. **Konfigurowanie terminarza zadań**

   Aby upewnić się, że lista aktualizacji jest zawsze aktualna, skonfiguruj terminarz zadania *Wyszukiwanie luk i wymaganych aktualizacji* tak, aby było uruchamiane automatycznie od czasu do czasu. Domyślna częstotliwość uruchamiania to raz na tydzień.

   Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej. Podczas konfigurowania terminarza zadania *Zainstaluj aktualizacje Windows Update* należy pamiętać, że dla tego zadania konieczne jest zdefiniowanie listy aktualizacji za każdym razem przed uruchomieniem tego zadania.

   Jeśli konfigurujesz terminarz uruchamiania zadań, upewnij się, że zadanie instalacji aktualizacji zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5. **Zatwierdzanie i odrzucanie aktualizacji oprogramowania (opcjonalne)**

   Jeśli utworzyłeś zadanie Zainstaluj wymagane aktualizacje i napraw luki, możesz określić reguły instalacji aktualizacji we właściwościach zadania. Jeśli utworzyłeś zadanie Zainstaluj aktualizacje Windows Update, pomiń ten krok.

   Dla każdej reguły możesz zdefiniować aktualizacje do zainstalowania w zależności od stanu aktualizacji: *Nie zdefiniowano*, *Zatwierdzono* lub *Odrzucono*. Na przykład, możesz utworzyć określone zadanie dla serwerów i ustawić regułę dla tego zadania, aby zezwolić na instalację tylko aktualizacji Windows Update i tylko tych, które posiadają stan *Zatwierdzono*. Po ręcznym ustawieniu stanu *Zatwierdzono* dla tych aktualizacji, które chcesz zainstalować. W tym przypadku aktualizacje Windows Update, które posiadają stan *Nie zdefiniowano* lub *Odrzucono*, nie będą zainstalowane na serwerach, które określiłeś w zadaniu.

   Używanie stanu *Zatwierdzone* do zarządzania instalacją aktualizacji jest wystarczające dla małej ilości uaktualnień. Aby zainstalować kilka aktualizacji, użyj reguł, które możesz skonfigurować w zadaniu *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzone* tylko dla tych określonych aktualizacji, które nie spełniają kryteriów określonych w regułach. Jeśli ręcznie zatwierdzisz dużą liczbę aktualizacji, wydajność Serwera administracyjnego ulegnie zmniejszeniu i może doprowadzić do przeciążenia Serwera administracyjnego.

   Domyślnie pobrane uaktualnienia oprogramowania posiadają stan *Niezdefiniowane*. Możesz zmienić stan na *Zatwierdzono* lub *Odrzucono* na liście **Aktualizacje oprogramowania** list (**Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**).

   Dostępne instrukcje:

   - Konsola administracyjna: Zatwierdzanie i odrzucanie aktualizacji oprogramowania
   - Kaspersky Security Center Web Console: Zatwierdzanie i odrzucanie aktualizacji oprogramowania innych firm

6. **Konfigurowanie Serwera administracyjnego do pracy jako serwer Windows Server Update Services (WSUS) (opcjonalne)**

   Domyślnie, aktualizacje Windows Update są pobierane na zarządzane urządzenia z serwerów Microsoft. Możesz zmienić to ustawienie, żeby używać Serwera administracyjnego jako serwera WSUS. W tym przypadku Serwer administracyjny synchronizuje dane aktualizacji z Windows Update w określonej częstotliwości i dostarcza aktualizacje w trybie scentralizowanym do Windows Update na urządzeniach w sieci.

   Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie Wykonaj synchronizację Windows Update i zaznacz pole **Użyj Serwera administracyjnego jako serwera WSUS** w zasadzie Agenta sieciowego.

   Dostępne instrukcje:

   - Konsola administracyjna: Synchronizowanie aktualizacji z Windows Update z Serwerem administracyjnym, Konfigurowanie aktualizacji systemu Windows w zasadzie Agenta sieciowego
   - Kaspersky Security Center Web Console: Tworzenie zadania synchronizacji Windows Update

7. **Uruchamianie zadania instalacji aktualizacji**

Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Zainstaluj aktualizacje Windows Update*. Jeśli uruchamiasz te zadania, aktualizacje są pobierane i instalowane na zarządzanych urządzeniach. Po zakończeniu zadania, upewnij się, że na liście zadań posiada stan *Zakończone pomyślnie*.

8. **Utwórz raport dotyczący wyników instalacji aktualizacji oprogramowania firm trzecich (opcjonalne)**

   Aby wyświetlić szczegółowe statystyki dotyczące instalacji aktualizacji, utwórz **Raport z wynikami instalacji aktualizacji oprogramowania firm trzecich**.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie i przeglądanie raportu
   - Kaspersky Security Center Web Console: Tworzenie i przeglądanie raportu

Wyniki

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, aktualizacje są automatycznie instalowane na zarządzanych urządzeniach. Jeśli nowe aktualizacje zostaną pobrane do repozytorium Serwera administracyjnego, Kaspersky Security Center sprawdzi, czy spełniają kryteria określone w regułach aktualizacji. Wszystkie nowe aktualizacje, które spełniają kryteria, zostaną zainstalowane automatycznie przy kolejnym uruchomieniu zadania.

Jeśli utworzyłeś zadanie *Zainstaluj aktualizacje Windows Update*, instalowane są tylko te aktualizacje określone we właściwościach zadania *Zainstaluj aktualizacje Windows Update*. W przyszłości, jeśli będziesz chciał zainstalować nowe aktualizacje pobrane do repozytorium Serwera administracyjnego, będziesz musiał dodać wymagane aktualizacje do listy aktualizacji w istniejącym zadaniu lub utworzyć nowe zadanie *Zainstaluj aktualizacje Windows Update*.

Przeglądanie informacji o dostępnych aktualizacjach aplikacji innych firm

W celu przejrzenia listy aktualizacji dostępnych dla aplikacji firm trzecich, zainstalowanych na urządzeniach klienckich:

W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.

W obszarze roboczym folderu możesz przejrzeć listę aktualizacji dostępnych dla aplikacji zainstalowanych na urządzeniach.

W celu przejrzenia właściwości aktualizacji:

W obszarze roboczym folderu **Aktualizacje oprogramowania**, z menu kontekstowego aktualizacji wybierz **Właściwości**.

W oknie właściwości aktualizacji można przeglądać następujące informacje:

- W sekcji **Ogólny** możesz wyświetlić **Stan zatwierdzenia aktualizacji**:
  - **Nie zdefiniowano** — aktualizacja jest dostępna na liście aktualizacji, ale nie została zatwierdzona do instalacji.
  - **Zatwierdzono** — aktualizacja jest dostępna na liście aktualizacji i zatwierdzona do instalacji.

- **Odrzucono** — instalacja aktualizacji została odrzucona.

- W sekcji **Atrybuty** możesz zobaczyć wartości pola **Zainstalowana automatycznie**:

  - Ta wartość **Automatycznie** jest wyświetlana, jeśli zadanie *Zainstaluj wymagane aktualizacje i napraw luki* może zainstalować aktualizacje dla aplikacji. Zadanie automatycznie instaluje nowe aktualizacje z adresu internetowego dostarczonego przez dostawcę oprogramowania innej firmy.

  - Ta wartość **Ręcznie** jest wyświetlana, jeśli Kaspersky Security Center nie może automatycznie zainstalować aktualizacji dla aplikacji. Aktualizacje można zainstalować ręcznie.

  To pole **Zainstalowana automatycznie** nie jest wyświetlane w przypadku aktualizacji aplikacji Windows.

- Listę urządzeń klienckich, dla których przeznaczona jest aktualizacja.

- Listę komponentów systemu (wymagania wstępne), które należy zainstalować przed aktualizacjami (jeśli istnieją).

- Luki w oprogramowaniu, które aktualizacja wyeliminuje.

Zatwierdzanie i odrzucanie aktualizacji oprogramowania

Ustawienia zadania instalacji aktualizacji mogą wymagać zatwierdzenia aktualizacji, które mają zostać zainstalowane. Możesz zatwierdzić uaktualnienia, które muszą zostać zainstalowane, oraz odrzucić uaktualnienia, które nie muszą zostać zainstalowane.

Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych aktualizacji na urządzeniach klienckich.

Używanie stanu *Zatwierdzone* do zarządzania instalacją aktualizacji firm trzecich jest wystarczające dla małej ilości uaktualnień. Aby zainstalować kilka aktualizacji innych firm, użyj reguł, które możesz skonfigurować w zadaniu *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzone* tylko dla tych określonych aktualizacji, które nie spełniają kryteriów określonych w regułach. Jeśli ręcznie zatwierdzisz dużą liczbę aktualizacji, wydajność Serwera administracyjnego ulegnie zmniejszeniu i może doprowadzić do przeciążenia Serwera administracyjnego.

W celu zatwierdzenia lub odrzucenia jednej lub kilku aktualizacji:

1. W drzewie konsoli wybierz węzeł **Zaawansowane → Zarządzanie aplikacjami → Aktualizacje oprogramowania**.

2. W obszarze roboczym folderu **Aktualizacje oprogramowania** kliknij przycisk **Odśwież** w prawym górnym rogu. Zostanie wyświetlona lista uaktualnień.

3. Wybierz uaktualnienia, które chcesz zatwierdzić lub odrzucić.

   W prawej części obszaru roboczego pojawi się okno z informacjami dla wybranych obiektów.

4. Z listy rozwijalnej **Stan zatwierdzenia aktualizacji** wybierz **Zatwierdzono**, aby zatwierdzić wybrane aktualizacje, lub **Odrzucono**, aby odrzucić wybrane aktualizacje.

   Domyślna wartość to **Nie zdefiniowano**.

Aktualizacje, dla których ustawiłeś stan **Zatwierdzono**, są umieszczane w kolejce do instalacji.

Aktualizacje, których ustawiony stan **Odrzucono**, są odinstalowywane (jeśli to możliwe) ze wszystkich urządzeń, na których były wcześniej zainstalowane. Dodatkowo, nie zostaną one zainstalowane na innych urządzeniach w przyszłości.

Niektórych uaktualnień dla aplikacji firmy Kaspersky nie można odinstalować. Jeśli ich ustawiony stan to **Odrzucono**, Kaspersky Security Center nie odinstaluje tych uaktualnień z urządzeń, na których były wcześniej zainstalowane. Jednakże te uaktualnienia nigdy nie zostaną zainstalowane na innych urządzeniach w przyszłości. Jeśli nie można odinstalować aktualizacji dla aplikacji Kaspersky, ta informacja zostanie wyświetlona w oknie właściwości aktualizacji: w panelu **Sekcje** wybierz **Ogólny**, a w obszarze roboczym ta informacja pojawi się w sekcji **Wymagania instalacyjne**. Jeśli ustawisz stan **Odrzucono** dla aktualizacji oprogramowania firm trzecich, te aktualizacje nie zostaną zainstalowane na urządzeniach, dla których planowane było ich zainstalowanie, ale jeszcze nie zostały zainstalowane. Uaktualnienia pozostaną na urządzeniach, na których zostały już zainstalowane. Jeśli musisz je usunąć, możesz je usunąć ręcznie lokalnie.

Synchronizacja aktualizacji z Windows Update z Serwerem administracyjnym

Jeśli w oknie **Ustawienia zarządzania aktualizacjami** kreatora wstępnej konfiguracji wybrano **Użyj Serwera administracyjnego jako serwera WSUS**, zadanie synchronizacji Windows Update zostanie utworzone automatycznie. Zadanie można uruchomić w folderze **Zadania**. Funkcja aktualizacji oprogramowania Microsoft jest dostępna tylko po pomyślnym zakończeniu zadania **Wykonaj synchronizację Windows Update**.

Zadanie **Wykonaj synchronizację Windows Update** pobiera tylko metadane z serwerów Microsoft. Jeśli sieć nie wykorzystuje serwera WSUS, każde urządzenie klienckie pobiera aktualizacje Microsoft niezależnie z zewnętrznych serwerów.

W celu utworzenia zadania synchronizacji Windows Updates z Serwerem administracyjnym:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.
2. Kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Konfiguruj synchronizację z usługą Windows Update**.

   Kreator tworzy zadanie **Wykonaj synchronizację Windows Update** wyświetlane w folderze **Zadania**.

   Zostanie uruchomiony kreator tworzenia zadania pobierania danych Centrum aktualizacji systemu Windows. Postępuj zgodnie z instrukcjami kreatora.

Zadanie synchronizacji Windows Update możesz również utworzyć w folderze **Zadania**, klikając **Utwórz zadanie**.

Microsoft regularnie usuwa przestarzałe aktualizacje z serwerów firmy, więc liczba bieżących aktualizacji zawsze mieści się pomiędzy 200 000, a 300 000. Aby zmniejszyć wykorzystanie miejsca na dysku i rozmiar bazy danych, Kaspersky Security Center usuwa nieaktualne aktualizacje, których nie ma już na serwerach aktualizacji firmy Microsoft.

Podczas wykonywania zadania **Wykonaj synchronizację Windows Update** aplikacja pobiera listę bieżących aktualizacji z serwera aktualizacji Microsoft. Następnie, Kaspersky Security Center tworzy listę aktualizacji, które są przestarzałe. Przy kolejnym uruchomieniu zadania **Wyszukiwanie luk i wymaganych aktualizacji** program Kaspersky Security Center oznaczy wszystkie przestarzałe aktualizacje i ustawi dla nich czas usunięcia. Przy kolejnym uruchomieniu zadania **Wykonaj synchronizację Windows Update** wszystkie aktualizacje, które zostały oznaczone do usunięcia 30 dni wcześniej, zostaną usunięte. Kaspersky Security Center sprawdza także obecność przestarzałych aktualizacji, które zostały oznaczone do usunięcia ponad 180 dni temu, a następnie usuwa te starsze aktualizacje.

Jeśli zadanie **Wykonaj synchronizację Windows Update** zostanie zakończone, a przestarzałe aktualizacje zostaną usunięte, baza danych może wciąż posiadać kody skrótów odnoszące się do plików usuniętych aktualizacji, a także odpowiednie pliki w plikach %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (jeśli zostały pobrane wcześniej). Możesz uruchomić zadanie **Konserwacja Serwera administracyjnego**, aby usunąć te przestarzałe wpisy z bazy danych oraz odpowiednie pliki.

Krok 1. Określanie, czy zmniejszyć ruch sieciowy

Jeśli Kaspersky Security Center synchronizuje aktualizacje z Microsoft Windows Update Servers, informacje o wszystkich plikach są zapisywane w bazie danych Serwera administracyjnego. Wszystkie pliki niezbędne dla aktualizacji zostają także pobrane na dysk podczas interakcji z Windows Update Agent. Kaspersky Security Center zapisuje informacje o plikach aktualizacji ekspresowej w bazie danych i pobiera je, gdy jest to konieczne. Pobranie plików aktualizacji ekspresowej prowadzi do zmniejszenia wolnego miejsca na dysku.

Aby uniknąć zmniejszenia ilości wolnego miejsca na dysku oraz zmniejszyć ruch sieciowy, możesz wyłączyć opcję **Pobierz ekspresowe pliki instalacyjne**.

Jeśli ta opcja jest zaznaczona, pliki aktualizacji ekspresowej są pobierane podczas wykonywania zadania. Domyślnie ta opcja nie jest zaznaczona.

Krok 2. Aplikacje

W tej sekcji możesz wybrać aplikacje, dla których zostaną pobrane uaktualnienia.

Jeśli pole **Wszystkie aplikacje** jest zaznaczone, uaktualnienia będą pobierane dla wszystkich istniejących aplikacji, a także dla wszystkich aplikacji, które mogą zostać wydane w przyszłości.

Domyślnie zaznaczone jest pole **Wszystkie aplikacje**.

Krok 3. Kategorie uaktualnień

W tej sekcji możesz wybrać kategorie uaktualnień, które będą pobierane na Serwer administracyjny.

Jeśli pole **Wszystkie kategorie** jest zaznaczone, uaktualnienia będą pobierane dla wszystkich istniejących kategorii uaktualnień, a także dla wszystkich kategorii, które mogą pojawić się w przyszłości.

Domyślnie zaznaczone jest pole **Wszystkie kategorie**.

Krok 4. Języki aktualizacji

W tym oknie możesz wybrać wersję językową aktualizacji, które są pobierane na Serwer administracyjny. Wybierz jedną z następujących opcji pobierania wersji językowych aktualizacji:

- **Pobierz wszystkie języki, wraz z nowymi**

  Jeśli ta opcja jest zaznaczona, na Serwer administracyjny zostaną pobrane wszystkie wersje językowe aktualizacji. Domyślnie opcja ta jest zaznaczona.

- **Pobierz wybrane języki**

  Jeśli ta opcja jest zaznaczona, z listy wersji językowych możesz wybrać te, które powinny zostać pobrane na Serwer administracyjny.

Krok 5. Wybieranie konta do uruchamiania zadania

W oknie **Wybieranie konta do uruchomienia zadania** możesz określić, które konto ma być używane podczas uruchamiania zadania. Wybierz jedną z następujących opcji:

- **Konto domyślne**

  Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

  Domyślnie opcja ta jest zaznaczona.

- **Określ konto**

  Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

  - **Konto**

    Konto, z poziomu którego zadanie jest uruchamiane.

  - **Hasło**

    Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

Krok 6. Konfigurowanie terminarza uruchamiania zadania

W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Zaplanowane uruchomienie:**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

- **Co N godzin**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

- **Co N dni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

  Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N tygodni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

  Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- **Co N minut**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

  Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Raz**

  Zadanie jest uruchamiane tylko raz, w określonym dniu i o określonej godzinie.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- **Uruchom pominięte zadania**

Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

Domyślnie opcja ta jest włączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

Krok 7. Definiowanie nazwy zadania

W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych (`"*<>?\:|`). Domyślna wartość to *Wykonaj synchronizację Windows Update*.

Krok 8. Kończenie tworzenia zadania

W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zakończyć pracę kreatora.

Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Nowo utworzone zadanie synchronizacji Windows Update pojawi się na liście zadań, w folderze **Zadania**.

Ręczne instalowanie uaktualnień na urządzeniach

Jeśli na stronie **Ustawienia zarządzania aktualizacjami** kreatora wstępnej konfiguracji wybrano **Wyszukaj i zainstaluj wymagane aktualizacje**, zadanie *instalacji wymaganych aktualizacji i napraw luk* zostanie utworzone automatycznie. Zadanie można uruchomić lub zatrzymać w folderze **Zarządzane urządzenia**, na zakładce **Zadania**.

Jeśli w kreatorze wstępnej konfiguracji wybrano **Wyszukaj wymagane aktualizacje**, możesz zainstalować aktualizacje oprogramowania na urządzeniach klienckich poprzez zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

Możesz wykonać jedną z następujących czynności:

- Utworzyć zadanie instalowania aktualizacji.
- Dodać regułę instalowania aktualizacji do istniejącego zadania instalowania aktualizacji.
- W ustawieniach istniejącego zadania instalacji aktualizacji skonfiguruj testową instalację aktualizacji.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Instalowanie aktualizacji poprzez utworzenie zadania instalacji

Możesz wykonać jedną z następujących czynności:

- Utworzyć zadanie instalowania pewnych aktualizacji.
- Wybierz aktualizację i utwórz zadanie jej instalowania i podobnych aktualizacji.

W celu zainstalowania określonych aktualizacji:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.
2. W obszarze roboczym wybierz aktualizacje, które chcesz zainstalować.
3. Wykonaj jedną z poniższych czynności:
   - Prawym klawiszem myszy kliknij wybrane aktualizacje na liście, a następnie wybierz **Zainstaluj aktualizację** → **Nowe zadanie**.
   - Kliknij odnośnik **Zainstaluj aktualizację (utwórz zadanie)** w oknie z informacjami dla wybranych aktualizacji.
4. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

   Zostanie uruchomiony kreator tworzenia zadania naprawy luk oraz instalacji aktualizacji. Postępuj zgodnie z krokami kreatora.

5. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** wybierz działanie, jakie zostanie wykonane, gdy system operacyjny na urządzeniach klienckich musi zostać uruchomiony ponownie po działaniu:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Uruchom ponownie po (min)**

    Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

    Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

Domyślnie opcja ta jest wyłączona.

6. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- Zaplanowane uruchomienie:

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - Co N godzin

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

  - Co N dni

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - Co N tygodni

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

    Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

  - Co N minut

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

  - Codziennie (czas letni nie jest obsługiwany)

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest włączona.

- Używaj automatycznie losowego opóźnienia dla uruchamiania zadań

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

7. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

8. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

   Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Zainstaluj wymagane aktualizacje i napraw luki** pojawi się w folderze **Zadania**.

We właściwościach zadania *instalacji wymaganych aktualizacj* i i naprawy luk można zezwolić na automatyczną instalację komponentów systemu (wymagania wstępne) przed instalacją aktualizacji. Jeśli ta opcja jest włączona, wszystkie wymagane komponenty systemu zostaną zainstalowane przed aktualizacją. Lista wymaganych komponentów znajduje się we właściwościach aktualizacji.

We właściwościach zadania *instalacji wymaganych aktualizacji* i naprawy luk można zezwolić na instalację aktualizacji, co spowoduje zaktualizowanie aplikacji do nowej wersji.

Jeśli w ustawieniach zadania znajdują się reguły instalacji aktualizacji firm trzecich, Serwer administracyjny pobierze wszystkie odpowiednie aktualizacje ze stron internetowych producentów. Aktualizacje są zapisywane w repozytorium Serwera administracyjnego, a następnie są rozsyłane i instalowane na urządzeniach, na których powinny zostać zastosowane.

Jeśli w ustawieniach zadania znajdują się reguły instalacji aktualizacji Microsoft, a Serwer administracyjny pełni rolę serwera WSUS, Serwer administracyjny pobierze wszystkie niezbędne aktualizacje do repozytorium, a następnie roześle je na zarządzane urządzenia. Jeśli sieć nie wykorzystuje serwera WSUS, każde urządzenie klienckie pobiera aktualizacje Microsoft niezależnie z zewnętrznych serwerów.

W celu zainstalowania określonej aktualizacji i jej podobnych:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.
2. W obszarze roboczym wybierz aktualizację, którą chcesz zainstalować.
3. Kliknij przycisk **Uruchom zadanie zdalnej instalacji**.

   Zostanie uruchomiony kreator instalacji aktualizacji.

   > Funkcje Kreator naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

   Postępuj zgodnie z krokami kreatora.
4. W oknie **Wyszukaj istniejące zadania instalacji aktualizacji** określ następujące ustawienia:

   - **Wyszukaj zadania, które instalują tę aktualizację**

     Jeśli ta opcja jest włączona, kreator instalacji aktualizacji wyszukuje istniejące zadania, które instalują wybraną aktualizację.

     Jeśli ta opcja jest wyłączona lub wyszukiwanie nie znajdzie stosowanych zadań, kreator instalacji aktualizacji wyświetli pytanie o utworzenie reguły lub zadania instalacji aktualizacji.

     Domyślnie opcja ta jest włączona.

   - **Zatwierdź instalację aktualizacji**

     Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

     Domyślnie opcja ta jest wyłączona.

5. Jeśli wybierzesz wyszukiwanie istniejących zadań instalacji aktualizacji i wyszukiwanie znajdzie zadania, możesz przejrzeć właściwości tych zadań lub uruchomić je ręcznie. Dalsze działania nie są wymagane.

   W przeciwnym razie kliknij przycisk **Nowe zadanie instalacji aktualizacji**.

6. Wybierz typ reguły instalacji, która ma zostać dodana do nowego zadania, a następnie kliknij przycisk **Zakończ**.

7. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

   Zostanie uruchomiony kreator tworzenia zadania naprawy luk oraz instalacji aktualizacji. Postępuj zgodnie z krokami kreatora.

8. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** wybierz działanie, jakie zostanie wykonane, gdy system operacyjny na urządzeniach klienckich musi zostać uruchomiony ponownie po działaniu:

   - Nie uruchamiaj ponownie urządzenia

     Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

   - Uruchom urządzenie ponownie

     Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

   - Pytaj użytkownika o akcję

     Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

     Domyślnie opcja ta jest zaznaczona.

     - Ponawiaj pytanie co (min)

       Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

       Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

       Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

     - Uruchom ponownie po (min)

Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- Wymuś zamknięcie aplikacji dla zablokowanych sesji

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

9. W oknie **Wybierz urządzenia, do których zostanie przypisane zadanie** wybierz jedną z następujących opcji:

- Wybierz urządzenia wykryte w sieci przez Serwer administracyjny

  Zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

  Na przykład, możesz chcieć użyć tej opcji w zadaniu instalowania Agenta sieciowego na nieprzypisanych urządzeniach.

- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy

  Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

  Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- Przypisz zadanie do wyboru urządzeń

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

- Przypisz zadanie do grupy administracyjnej

Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

10. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Zaplanowane uruchomienie:**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - **Co N godzin**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

  - **Co N dni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - **Co N tygodni**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

    Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

  - **Co N minut**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

  - **Codziennie (czas letni nie jest obsługiwany)**

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie** (zaznaczone domyślnie)

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest włączona.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

11. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

12. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

    Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Zainstaluj wymagane aktualizacje i napraw luki** jest tworzone i wyświetlane w folderze **Zadania**.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Aktualizacja do nowej wersji aplikacji może spowodować problemy z działaniem niektórych aplikacji na urządzeniach.

Instalowanie aktualizacji poprzez dodanie reguły do istniejącego zadania instalacji

W celu zainstalowania aktualizacji poprzez dodanie reguły do istniejącego zadania instalacji:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Aktualizacje oprogramowania**.
2. W obszarze roboczym wybierz aktualizację, którą chcesz zainstalować.
3. Kliknij przycisk **Uruchom zadanie zdalnej instalacji**.

   Zostanie uruchomiony kreator instalacji aktualizacji.

   Funkcje Kreator naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

   Postępuj zgodnie z krokami kreatora.
4. W oknie **Wyszukaj istniejące zadania instalacji aktualizacji** określ następujące ustawienia:
   - **Wyszukaj zadania, które instalują tę aktualizację**

     Jeśli ta opcja jest włączona, kreator instalacji aktualizacji wyszukuje istniejące zadania, które instalują wybraną aktualizację.

     Jeśli ta opcja jest wyłączona lub wyszukiwanie nie znajdzie stosowanych zadań, kreator instalacji aktualizacji wyświetli pytanie o utworzenie reguły lub zadania instalacji aktualizacji.

     Domyślnie opcja ta jest włączona.
   - **Zatwierdź instalację aktualizacji**

     Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

     Domyślnie opcja ta jest wyłączona.
5. Jeśli wybierzesz wyszukiwanie istniejących zadań instalacji aktualizacji i wyszukiwanie znajdzie zadania, możesz przejrzeć właściwości tych zadań lub uruchomić je ręcznie. Dalsze działania nie są wymagane.

   W innej sytuacji kliknij przycisk **Dodaj regułę instalacji aktualizacji**.
6. Wybierz zadanie, do którego chcesz dodać regułę, a następnie kliknij przycisk **Dodaj regułę**.

Możesz także przejrzeć właściwości istniejących zadań, uruchomić je ręcznie lub utworzyć nowe zadanie.

7. Wybierz typ reguły, która zostanie dodana do wybranego zadania, a następnie kliknij przycisk **Zakończ**.

8. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

Nowa reguła instalacji aktualizacji zostanie dodana do istniejącego zadania **Instalacja wymaganych aktualizacji i naprawa luk**.

Konfigurowanie testowej instalacji aktualizacji

W celu skonfigurowania testowej instalacji aktualizacji:

1. W drzewie konsoli wybierz zadanie **Zainstaluj wymagane aktualizacje i napraw luki** znajdujące się w folderze **Zarządzane urządzenia**, na zakładce **Zadania**.

2. Z menu kontekstowego zadania wybierz **Właściwości**.

   Zostanie otwarte okno właściwości **Zainstaluj wymagane aktualizacje i napraw luki**.

3. W oknie właściwości zadania, w sekcji **Instalacja testowa** wybierz jedną z opcji dostępnych dla instalacji testowej:

   - **Nie skanuj**. Wybierz tę opcję, jeśli nie chcesz przeprowadzać testowej instalacji aktualizacji.

   - **Uruchom skanowanie na wybranych urządzeniach**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na wybranych urządzeniach. Kliknij przycisk **Dodaj** i wybierz urządzenia, na których chcesz przeprowadzić testową instalację aktualizacji.

   - **Uruchom skanowanie na urządzeniach w określonej grupie**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na grupach urządzeń. W polu **Określ grupę testową** określ grupę urządzeń, na których chcesz przeprowadzić instalację testową.

   - **Uruchom skanowanie na określonym procencie urządzeń**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na określonej liczbie urządzeń. W polu **Procentowy udział urządzeń testowych z wszystkich urządzeń docelowych** określ procentową ilość urządzeń, na których chcesz przeprowadzić testową instalację aktualizacji.

4. Po wybraniu dowolnej opcji, za wyjątkiem **Nie skanuj**, w polu **Czas na podjęcie decyzji, jeśli instalacja ma być kontynuowana, w godzinach** określ liczbę godzin, jaka powinna upłynąć od testowej instalacji aktualizacji do momentu uruchomienia instalacji aktualizacji na wszystkich urządzeniach.

Konfigurowanie aktualizacji systemu Windows w profilu Agenta sieciowego

W celu skonfigurowania aktualizacji systemu Windows w profilu Agenta sieciowego:

1. W drzewie konsoli wybierz **Zarządzane urządzenia**.

2. W obszarze roboczym wybierz zakładkę **Zasady**.

3. Wybierz profil Agenta sieciowego.

4. Z otwartego menu kontekstowego zasady wybierz **Właściwości**.

   Zostanie otwarte okno właściwości profilu Agenta sieciowego.

5. W panelu **Sekcje** wybierz **Aktualizacje oprogramowania i luki**.

6. Zaznacz opcję **Użyj Serwera administracyjnego jako serwera WSUS**, aby pobierać aktualizacje systemu Windows na Serwer administracyjny, a następnie rozsyłać je na urządzenia klienckie przy użyciu Agenta sieciowego.

   Jeśli ta opcja nie jest zaznaczona, aktualizacje systemu Windows nie są pobierane na Serwer administracyjny. W tym przypadku urządzenia klienckie pobierają aktualizacje systemu Windows bezpośrednio z serwerów firmy Microsoft.

7. Wybierz zestaw aktualizacji, które użytkownicy mogą zainstalować na swoich urządzeniach ręcznie, korzystając z Windows Update.

   Na urządzeniach działających pod kontrolą systemu Windows 10, jeśli usługa Windows Update już wykryła aktualizacje dla urządzenia, nowa opcja, którą wybierzesz w sekcji **Zezwalaj użytkownikom na zarządzanie instalowaniem aktualizacji Windows Update**, zostaną zastosowane dopiero po zainstalowaniu wykrytych aktualizacji.

   Wybierz element z listy rozwijalnej:

   - Zezwalaj użytkownikom na instalację wszystkich dostępnych aktualizacji Windows Update

     Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach.

     Wybierz tę opcję, jeśli nie chcesz uczestniczyć w instalacji aktualizacji.

     Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

   - Zezwalaj użytkownikom na instalację wszystkich zatwierdzonych aktualizacji Windows Update

     Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach i które zostały zatwierdzone przez Ciebie.

     Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych zatwierdzonych aktualizacji.

     Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

   - Nie zezwalaj użytkownikom na instalowanie aktualizacji Windows Update

Użytkownicy nie mogą ręcznie zainstalować aktualizacji Microsoft Windows Update na swoich urządzeniach. Wszystkie stosowane aktualizacje są instalowane w sposób skonfigurowany przez Ciebie.

Wybierz tę opcję, jeśli chcesz zarządzać instalacją aktualizacji w sposób scentralizowany.

Na przykład, możesz chcieć zoptymalizować terminarz aktualizacji, aby sieć nie została przeciążona. Możesz skonfigurować terminarz aktualizacji po godzinach, aby nie przeszkadzały w pracy użytkowników.

8. Wybierz tryb szukania aktualizacji systemu Windows:

- **Aktywny**

  Jeśli ta opcja jest zaznaczona, Serwer administracyjny z pomocą Agenta sieciowego przesyła żądanie z Agenta Windows Update na urządzeniu klienckim do źródła uaktualnień: Serwery Windows Update lub WSUS. Następnie Agent sieciowy przesyła informacje z usługi Windows Update Agent do Serwera administracyjnego.

  Opcja zaczyna działać tylko wtedy, gdy zaznaczona jest opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

  Domyślnie opcja ta jest zaznaczona.

- **Pasywny**

  Jeżeli ta opcja jest zaznaczona, Agent sieciowy co jakiś czas przesyła informacje od Serwera administracyjnego dotyczące aktualizacji pobranych przy ostatniej synchronizacji agenta usługi Windows Update ze źródłem uaktualnień. Jeśli nie zostanie przeprowadzona synchronizacja agenta usługi Windows Update ze źródłem uaktualnień, informacje o aktualizacjach Serwera administracyjnego będą przestarzałe.

  Wybierz tę opcję, jeśli chcesz uzyskać aktualizacje z pamięci podręcznej źródła uaktualnień.

- **Wyłączono**

  Jeśli ta opcja jest zaznaczona, Serwer administracyjny nie żąda informacji dotyczących aktualizacji.

  Wybierz tę opcję, gdy, na przykład, chcesz najpierw przetestować aktualizacje na swoim lokalnym urządzeniu.

9. Zaznacz opcję **Skanuj pliki wykonywalne w poszukiwaniu luk podczas ich uruchamiania**, jeśli chcesz skanować pliki wykonywalne w poszukiwaniu luk podczas uruchamiania plików.

10. Upewnij się, że edycja jest zablokowana dla wszystkich zmienionych ustawień. W przeciwnym razie zmiany nie mają zastosowania.

11. Kliknij **Zastosuj**.

Eliminowanie luk w oprogramowaniu innych firm

Ta sekcja opisuje funkcje Kaspersky Security Center, które dotyczą eliminowania luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach.

Scenariusz: Wyszukiwanie i usuwanie luk w oprogramowaniu firm trzecich

Ta sekcja zawiera scenariusz wyszukiwania i naprawiania luk na zarządzanych urządzeniach działających pod kontrolą systemu Windows. Możesz znaleźć i naprawić luki w oprogramowaniu w systemie operacyjnym oraz w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft.

Wymagania wstępne

- Kaspersky Security Center zostanie wdrożony w Twojej organizacji.
- W Twojej organizacji znajdują się zarządzane urządzenia działające pod kontrolą systemu Windows.
- Połączenie internetowe w przypadku Serwera administracyjnego jest wymagane, aby można było wykonywać następujące zadania:
  - Sporządzanie listy zalecanych poprawek dla luk w oprogramowaniu firmy Microsoft. Lista jest tworzona i regularnie aktualizowana przez specjalistów z Kaspersky.
  - Naprawianie luk w oprogramowaniu firm trzecich innym niż oprogramowanie firmy Microsoft.

Etapy

Wyszukiwanie i naprawianie luk w oprogramowaniu odbywa się w etapach:

1. **Skanowanie luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach**

   Aby odszukać luki w oprogramowaniu zainstalowanym na zarządzanych urządzeniach, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

   Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Jeśli nie uruchamiałeś kreatora, uruchom go teraz lub utwórz zadanie ręcznie.

   Dostępne instrukcje:

   - Konsola administracyjna: Skanowanie aplikacji w poszukiwaniu luk, Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console: Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji, Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

2. **Analizowanie listy wykrytych luk w oprogramowaniu**

   Przejrzyj listę **Luki w oprogramowaniu** i zdecyduj, które luki mają zostać naprawione. Aby przejrzeć szczegółowe informacje o każdej luce, kliknij nazwę luki na liście. Dla każdej luki na liście możesz także przejrzeć statystyki dotyczące luki na zarządzanych urządzeniach.

   Dostępne instrukcje:

   - Konsola administracyjna: Przeglądanie informacji o lukach w oprogramowaniu, Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

- Kaspersky Security Center Web Console: Przeglądanie informacji o lukach w oprogramowaniu, Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

3. **Konfigurowanie naprawy luk**

   Jeśli luki w oprogramowaniu zostaną wykryte, możesz naprawić luki w oprogramowaniu na zarządzanych urządzeniach, korzystając z zadania *Zainstaluj wymagane aktualizacje i napraw luki* lub zadania *Napraw luki*.

   Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft, zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawę kilku luk zgodnie z pewnymi regułami. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami. Aby naprawić luki w oprogramowaniu, zadanie *Zainstaluj wymagane aktualizacje i napraw luki* używa zalecanych aktualizacji oprogramowania.

   Zadanie *Napraw luki* nie wymaga opcji licencjonowania dla funkcji Zarządzanie lukami i poprawkami. Aby użyć tego zadania, należy ręcznie określić poprawki użytkownika dla luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla programów innych firm.

   Możesz uruchomić Kreator naprawiania luk, który tworzy jedno z tych zadań automatycznie, lub możesz utworzyć jedno z tych zadań ręcznie.

   Dostępne instrukcje:

   - Konsola administracyjna: Wybieranie poprawek użytkownika dla luk w programach innych firm, Naprawianie luk w aplikacjach
   - Kaspersky Security Center Web Console: Wybieranie poprawek użytkownika dla luk w programach innych firm, Naprawianie luk w programach innych firm, Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki

4. **Konfigurowanie terminarza zadań**

   Aby upewnić się, że lista luk jest zawsze aktualna, skonfiguruj zadanie *Wyszukiwanie luk i wymaganych aktualizacji* tak, aby było uruchamiane automatycznie od czasu do czasu. Zalecana przeciętna częstotliwość uruchamiania to raz na tydzień.

   Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej. Podczas ustawiania terminarza zadania *Napraw luki* należy pamiętać, żeby wybrać poprawki dla oprogramowania Microsoft lub określić poprawki użytkownika dla oprogramowania innych firm za każdym razem przed rozpoczęciem zadania.

   Jeśli konfigurujesz terminarz uruchamiania zadania, upewnij się, że zadanie naprawy luki zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5. **Ignorowanie luk w oprogramowaniu (opcjonalne)**

   Jeśli chcesz, możesz zignorować luki w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

   Dostępne instrukcje:

   - Konsola administracyjna: Ignorowanie luk w oprogramowaniu
   - Kaspersky Security Center Web Console: Ignorowanie luk w oprogramowaniu

6. **Uruchamianie zadania naprawy luk**

   Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Napraw lukę*. Po zakończeniu zadania, upewnij się, że na liście zadań posiada stan *Zakończone pomyślnie*.

7. **Utwórz raport dotyczący wyników naprawy luk w oprogramowaniu (opcjonalne)**

Aby wyświetlić szczegółowe statystyki dotyczące naprawy luk, wygeneruj Raport o lukach. Raport wyświetla informacje o lukach w oprogramowaniu, które nie zostały naprawione. Dzięki temu możesz wiedzieć o wyszukiwaniu i naprawie luk w programach innych firm, w tym w oprogramowaniu firmy Microsoft, w swojej organizacji.

Dostępne instrukcje:

- Konsola administracyjna: Tworzenie i przeglądanie raportu
- Kaspersky Security Center Web Console: Tworzenie i przeglądanie raportu

8. **Sprawdzanie konfiguracji wyszukiwania i naprawy luk w programach innych firm**

   Upewnij się, że wykonałeś następujące czynności:

   - Uzyskałeś i przejrzałeś listę luk w oprogramowaniu na zarządzanych urządzeniach
   - Zignorowałeś luki w oprogramowaniu, jeśli chciałeś
   - Skonfigurowałeś zadanie naprawy luk
   - Skonfigurowałeś terminarz zadań wyszukiwania i naprawy luk w oprogramowaniu, aby były uruchamianie po kolei
   - Sprawdziłeś, czy zadanie naprawy luk w oprogramowaniu zostało uruchomione

Wyniki

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, luki zostają naprawione na zarządzanych urządzeniach automatycznie. Jeśli zadanie zostaje uruchomione, zestawia listę dostępnych aktualizacji oprogramowania z regułami określonymi w ustawieniach zadania. Wszystkie aktualizacje oprogramowania, które spełniają kryteria w regułach, zostaną pobrane do repozytorium Serwera administracyjnego i zostaną zainstalowane w celu naprawy luk w oprogramowaniu.

Jeśli utworzyłeś zadanie *Napraw luki*, naprawione zostaną tylko luki w oprogramowaniu firmy Microsoft.

Informacje o wyszukiwaniu i eliminowaniu luk w oprogramowaniu

Kaspersky Security Center wykrywa i naprawia luki w oprogramowaniu na zarządzanych urządzeniach działających pod kontrolą systemów operacyjnych z rodziny Microsoft Windows. Luki są wykrywane w systemie operacyjnym i w oprogramowaniu innych firm, w tym w oprogramowaniu firmy Microsoft.

Wyszukiwanie luk w oprogramowaniu

Aby znaleźć luki w oprogramowaniu, Kaspersky Security Center wykorzystuje znaki charakterystyczne z bazy danych znanych zagrożeń. Ta baza danych jest tworzona przez specjalistów z Kaspersky. Zawiera informacje o lukach, takie jak opis luki, data wykrycia luki, priorytet luki. Szczegóły dotyczące luk w oprogramowaniu można znaleźć na stronie internetowej Kaspersky.

Kaspersky Security Center wykorzystuje zadanie *Wyszukiwanie luk i wymaganych aktualizacji* do wykrywania luk w oprogramowaniu.

Naprawianie luk w oprogramowaniu

Aby naprawić luki w oprogramowaniu, Kaspersky Security Center używa aktualizacji oprogramowania opublikowanych przez producentów oprogramowania. Metadane aktualizacji oprogramowania są pobierane z repozytorium Serwera administracyjnego w wyniku uruchomienia następującego zadania:

- *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. To zadanie jest przeznaczone do pobrania metadanych aktualizacji dla Kaspersky i oprogramowania firm trzecich. To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Możesz ręcznie utworzyć zadanie Pobierz uaktualnienia do repozytorium Serwera administracyjnego.

- *Wykonaj synchronizację Windows Update*. To zadanie jest przeznaczone do pobrania metadanych aktualizacji dla oprogramowania firmy Microsoft.

Aktualizacje oprogramowania eliminujące luki mogą być w postaci pełnych pakietów dystrybucyjnych lub poprawek. Aktualizacje oprogramowania, które eliminują luki w oprogramowaniu, nazywane są *poprawkami*. *Zalecane poprawki* to takie poprawki, które są zalecane do zainstalowania przez specjalistów z Kaspersky. *Poprawki użytkownika* to takie poprawki, które są ręcznie określane do zainstalowania przez użytkowników. Aby zainstalować poprawkę użytkownika, należy utworzyć pakiet instalacyjny zawierający tę poprawkę.

Jeśli posiadasz licencję dla Kaspersky Security Center z funkcją Zarządzanie lukami i poprawkami, aby usunąć luki w oprogramowaniu, możesz użyć zadania *Zainstaluj wymagane aktualizacje i napraw luki*. To zadanie automatycznie eliminuje kilka luk poprzez zainstalowanie zalecanych poprawek. Dla tego zadania można ręcznie skonfigurować pewne reguły do naprawy kilku luk.

Jeśli nie posiadasz licencji dla Kaspersky Security Center z funkcją Zarządzanie lukami i poprawkami, aby usunąć luki w oprogramowaniu, możesz użyć zadania *Napraw luki*. Korzystając z tego zadania, możesz wyeliminować luki poprzez zainstalowanie zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu złośliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk w zabezpieczeniach (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Aby naprawić niektóre luki w oprogramowaniu, należy zaakceptować Umowę licencyjną (EULA) dla instalowanego oprogramowania, jeśli wymagane jest zaakceptowanie Umowy licencyjnej. Jeśli odrzucisz Umowę licencyjną, luka w oprogramowaniu nie zostanie wyeliminowana.

Przeglądanie informacji o lukach w oprogramowaniu

W celu przejrzenia listy luk wykrytych na urządzeniach klienckich:

W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

Strona wyświetla listę luk w aplikacjach wykrytych na zarządzanych urządzeniach.

W celu uzyskania informacji o wybranej luce:

Z menu kontekstowego luki wybierz **Właściwości**.

Zostanie otwarte okno właściwości luki, wyświetlające następujące informacje:

- Aplikacja, w której wykryto lukę.
- Lista urządzeń, na których wykryto lukę.
- Informacje dotyczące naprawy luki.

W celu wyświetlenia raportu o wszystkich wykrytych lukach:

W folderze **Luki w oprogramowaniu** kliknij odnośnik **Wyświetl raport o lukach**.

Zostanie utworzony raport o lukach w aplikacjach zainstalowanych na urządzeniach. Możesz wyświetlić ten raport w węźle z nazwą odpowiedniego Serwera administracyjnego, otwierając zakładkę **Raporty**.

Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

Statystyki dla każdej luki w oprogramowaniu możesz przejrzeć na zarządzanych urządzeniach. Statystyki są przedstawiane w postaci wykresu. Wykres wyświetla liczbę urządzeń z następującymi stanami:

- *Zignorowano na: <liczba urządzeń>*. Stan jest przypisywany, jeśli we właściwościach luki ręcznie ustawiłeś opcję ignorowania luki.
- *Naprawiono na: <liczba urządzeń>*. Stan jest przypisywany, jeśli zadanie naprawy luki zostało zakończone pomyślnie.
- *Naprawa zaplanowana na: <liczba urządzeń>*. Stan jest przypisywany, jeśli utworzyłeś zadanie naprawy luki, ale zadanie nie zostało jeszcze wykonane.
- *Zastosowano poprawkę na: <liczba urządzeń>*. Stan jest przypisywany, jeśli ręcznie wybrałeś aktualizację oprogramowania do naprawy luki, ale ta aktualizacja oprogramowania nie usunęła luki.
- *Naprawa wymagana na: <liczba urządzeń>*. Stan jest przypisywany, jeśli luka została naprawiona tylko na części zarządzanych urządzeń, a wymagana jest jej naprawa na reszcie zarządzanych urządzeń.

W celu sprawdzenia statystyk dotyczących luki na zarządzanych urządzeniach:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

   Strona wyświetla listę luk w aplikacjach wykrytych na zarządzanych urządzeniach.

2. Wybierz lukę, dla której chcesz przejrzeć statystyki.

W sekcji do pracy z wybranym obiektem wyświetlany jest wykres stanów luki. Kliknięcie stanu spowoduje otwarcie listy urządzeń, na których luka posiada wybrany stan.

Skanowanie aplikacji w poszukiwaniu luk

Jeśli skonfigurowano aplikację poprzez Kreator wstępnej konfiguracji, zadanie *Wykrywanie* luk zostanie utworzone automatycznie. Zadanie można zobaczyć w folderze **Zarządzane urządzenia**, na zakładce **Zadania**.

W celu utworzenia zadania wykrywania luk w aplikacjach zainstalowanych na urządzeniach klienckich:

1. W drzewie konsoli wybierz **Zaawansowane** → **Zarządzanie aplikacjami**, a następnie wybierz podfolder **Luki w oprogramowaniu**.

2. W obszarze roboczym wybierz **Akcje dodatkowe** → **Konfiguruj wykrywanie luk**.

   Jeśli zadanie wykrywania luk już istnieje, zostanie wyświetlona zakładka **Zadania** folderu **Zarządzane urządzenia** z wybranym istniejącym zadaniem. W przeciwnym razie zostanie uruchomiony kreator tworzenia zadania usuwania luk w zabezpieczeniach. Postępuj zgodnie z krokami kreatora.

3. W oknie **Wybierz typ zadania** wybierz **Wyszukiwanie luk i wymaganych aktualizacji**.

4. W oknie **Ustawienia** określ ustawienia zadania w następujący sposób:

   - Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft

     Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

     Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

     Domyślnie opcja ta jest włączona.

   - Połącz z serwerem aktualizacji, aby zaktualizować dane

Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł uaktualnień Microsoft:

- Serwer administracyjny Kaspersky Security Center (zapoznaj się z ustawieniami profilu Agenta sieciowego)
- System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
- Serwery aktualizacji Microsoft

Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła uaktualnień Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach profilu Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

Domyślnie opcja ta jest włączona.

Kombinacja następujących opcji ustawień profilu Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

- Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie z serwerem aktualizacji, aby uzyskać aktualizacje tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona, a opcja **Aktywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została zaznaczona.
- Agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła uaktualnień Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia, jeśli opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** została włączona, a opcja **Pasywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została wybrana, jeśli opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest wyłączona, a opcja **Aktywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została zaznaczona.
- Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Wyłączono** w ustawieniach grupy **Tryb wyszukiwania aktualizacji systemu Windows** jest zaznaczona, Kaspersky Security Center nie żąda żadnych informacji o aktualizacjach.

- Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky

Jeśli ta opcja jest włączona, Kaspersky Security Center wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

Domyślnie opcja ta jest włączona.

- **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**

  Foldery, w których Kaspersky Security Center wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

  Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

5. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

   - **Zaplanowane uruchomienie:**

     Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

   - **Co N godzin**

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

- **Co N dni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

  Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N tygodni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

  Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- **Co N minut**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

  Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po pobraniu nowych uaktualnień do repozytorium**

  Zadanie jest uruchamiane po pobraniu uaktualnień do repozytorium. Na przykład, możesz użyć tego terminarza dla zadania wyszukiwania luk i wymaganych aktualizacji.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- **Uruchom pominięte zadania**

Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

Domyślnie opcja ta jest włączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

6. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

7. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

   Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Wyszukiwanie luk** i wymaganych aktualizacji pojawi się na liście zadań w folderze **Zarządzane urządzenia**, na zakładce **Zadania**.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Po zakończeniu zadania *Wyszukiwanie luk* i wymaganych aktualizacji, Serwer administracyjny wyświetla listę luk wykrytych w aplikacjach zainstalowanych na urządzeniu; wyświetla także wszystkie aktualizacje oprogramowania wymagane do wyeliminowania wykrytych luk.

Jeśli wyniki zadania zawierają błąd agenta usługi Windows Update 0x80240033 „Windows Update Agent error 80240033 ("License terms could not be downloaded.")" („pobranie warunków licencyjnych nie powiodło się"), możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

Serwer administracyjny nie wyświetla listy wymaganych aktualizacji oprogramowania, jeśli uruchamiasz dwa zadania po kolei — zadanie *Wykonaj synchronizację Windows Update* ma wyłączoną opcję **Pobierz pliki instalacji ekspresowej**, a następnie zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Aby przejrzeć listę wymaganych aktualizacji oprogramowania, musisz ponownie uruchomić zadanie *Wyszukiwanie luk i wymaganych aktualizacji*.

Agent sieciowy otrzymuje informacje o wszelkich dostępnych aktualizacjach systemu Windows i aktualizacjach dla innych produktów Microsoft od Windows Update lub Serwera administracyjnego, gdy Serwer administracyjny pełni rolę serwera WSUS. Informacje są przesyłane, gdy aplikacje zostają uruchomione (jeśli jest to dostępne dla profilu) i przy każdym uruchomieniu zadania *Wyszukiwanie luk* i wymaganych aktualizacji na urządzeniach klienckich.

Szczegółowe informacje dotyczące oprogramowania firm trzecich, które może być aktualizowane poprzez Kaspersky Security Center, można znaleźć na stronie działu pomocy technicznej, na podstronie poświęconej Kaspersky Security Center, w sekcji **Zarządzanie serwerem**.

Naprawianie luk w aplikacjach

Jeśli na stronie **Ustawienia zarządzania aktualizacjami** kreatora wstępnej konfiguracji wybrano **Wyszukaj i zainstaluj wymagane aktualizacje**, zadanie *instalacji wymaganych aktualizacji i napraw luk* zostanie utworzone automatycznie. Zadanie jest wyświetlane w obszarze roboczym folderu **Zarządzane urządzenia**, na zakładce **Zadania**.

Jeśli jest inaczej, możesz wykonać jedną z następujących czynności:

- Utwórz zadanie naprawy luk poprzez zainstalowanie dostępnych uaktualnień.
- Dodaj regułę dla naprawy luk do istniejącego zadania naprawy luk.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Naprawianie luk poprzez utworzenie zadania naprawy luk

Możesz wykonać jedną z następujących czynności:

- Utwórz zadanie naprawy kilku luk, które spełniają określone reguły.
- Wybierz lukę i utwórz zadanie naprawy tej luki i podobnych luk.

W celu naprawy luk, które spełniają określone reguły:

1. W drzewie konsoli wybierz Serwer administracyjny na urządzeniach, których luki chcesz naprawić.
2. W menu **Widok** okna głównego aplikacji wybierz **Konfiguruj interfejs**.
3. W oknie, które zostanie otwarte, zaznacz pole wyboru **Wyświetl zarządzanie lukami i poprawkami**, a następnie kliknij przycisk **OK**.
4. W oknie z wiadomością aplikacji kliknij **OK**.
5. Uruchom ponownie Konsolę administracyjną, aby zmiany zostały zastosowane.
6. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
7. W obszarze roboczym wybierz zakładkę **Zadania**.
8. Kliknij przycisk **Utwórz zadanie**, aby uruchomić Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
9. W oknie **Wybierz typ zadania** wybierz **Zainstaluj wymagane aktualizacje i napraw luki**.

   Jeśli zadanie nie jest wyświetlane, sprawdź, czy Twoje konto ma uprawnienia **Odczyt**, **Modyfikuj** i **Wykonaj** dla obszaru funkcjonalnego **Zarządzanie systemem: Zarządzanie lukami w zabezpieczeniach i poprawkami**. Bez tych praw dostępu nie można utworzyć ani skonfigurować zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
10. W oknie **Ustawienia** określ ustawienia zadania w następujący sposób:

    - **Określ reguły instalacji aktualizacji**

      Te reguły są stosowane do instalacji aktualizacji na urządzeniach klienckich. Jeśli reguły nie zostały określone, zadanie nie zostanie wykonane. Informacje dotyczące działań wykonywanych na regułach znajdziesz w sekcji Reguły instalacji aktualizacji.

    - **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia**

      Jeśli ta opcja jest włączona, aktualizacje są instalowane po ponownym uruchomieniu lub zamknięciu urządzenia. W innym przypadku aktualizacje są instalowane zgodnie z terminarzem.

      Użyj tej opcji, jeśli instalowanie aktualizacji może wpłynąć na działanie urządzenia.

      Domyślnie opcja ta jest wyłączona.

    - **Zainstaluj wymagane ogólne składniki systemu**

      Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

      Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

      Domyślnie opcja ta jest wyłączona.

    - **Zezwól na instalację nowych wersji aplikacji podczas aktualizacji**

Jeśli ta opcja jest włączona, aktualizacje są dozwolone, gdy powodują zainstalowanie nowej wersji aplikacji.

Jeśli ta opcja jest wyłączona, aplikacja nie zostanie zaktualizowana. W takiej sytuacji możesz ręcznie zainstalować nowe wersje aplikacji lub użyć w tym celu innego zadania. Na przykład, możesz użyć tej opcji, jeśli struktura Twojej firmy nie jest obsługiwana przez nową wersję aplikacji lub jeśli chcesz sprawdzić aktualizację w infrastrukturze testowej.

Domyślnie opcja ta jest włączona.

Aktualizowanie aplikacji może spowodować problemy z działaniem powiązanych aplikacji zainstalowanych na urządzeniach klienckich.

- Pobierz aktualizacje na urządzenie, ale ich nie instaluj

  Jeśli ta opcja jest włączona, aplikacja pobierze uaktualnienia na urządzenie, ale nie zainstaluje ich automatycznie. Możesz ręcznie zainstalować pobrane aktualizacje.

  Aktualizacje Microsoft są pobierane do folderu systemowego Windows. Aktualizacje aplikacji firm trzecich (aplikacje innych producentów niż Kaspersky i Microsoft) są pobierane do folderu określonego w polu **Folder do pobierania aktualizacji**.

  Jeśli ta opcja jest wyłączona, aktualizacje są instalowane na urządzeniu automatycznie.

  Domyślnie opcja ta jest wyłączona.

  - Folder do pobierania aktualizacji

    Ten folder jest używany do pobierania aktualizacji aplikacji innych firm (aplikacji innych producentów niż Kaspersky i Microsoft).

- Włącz diagnostykę zaawansowaną

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

  - Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB

    Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

11. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** wybierz działanie, jakie zostanie wykonane, gdy system operacyjny na urządzeniach klienckich musi zostać uruchomiony ponownie po działaniu:

- Nie uruchamiaj ponownie urządzenia

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- Uruchom urządzenie ponownie

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- Pytaj użytkownika o akcję

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - Ponawiaj pytanie co (min)

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - Uruchom ponownie po (min)

    Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

    Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- Wymuś zamknięcie aplikacji dla zablokowanych sesji

Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

Domyślnie opcja ta jest wyłączona.

12. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- Zaplanowane uruchomienie:

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - Co N godzin

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

  - Co N dni

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - Co N tygodni

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

    Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

  - Co N minut

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

  - Codziennie (czas letni nie jest obsługiwany)

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest włączona.

- Używaj automatycznie losowego opóźnienia dla uruchamiania zadań

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

13. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

14. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

    Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Zainstaluj wymagane aktualizacje i napraw luki** jest tworzone i wyświetlane w folderze **Zadania**.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Jeśli wyniki zadania zawierają błąd agenta usługi Windows Update 0x80240033 „Windows Update Agent error 80240033 ("License terms could not be downloaded.")" („pobranie warunków licencyjnych nie powiodło się"), możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

W celu naprawy określonej luki i jej podobnych:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.
2. Wybierz lukę, którą chcesz naprawić.
3. Kliknij przycisk **Uruchom kreatora naprawiania luk**.

   Zostanie uruchomiony Kreator naprawiania luk.

   Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

   Postępuj zgodnie z krokami kreatora.
4. W oknie **Wyszukaj istniejące zadania naprawiania luk** określ następujące parametry:

   - **Pokaż tylko zadania naprawiające tę lukę**

     Jeśli ta opcja jest wyłączona, Kreator naprawiania luk wyszukuje istniejące zadania, które naprawiają wybraną lukę.

     Jeśli ta opcja jest wyłączona lub wyszukiwanie nie znajdzie stosowanych zadań, Kreator naprawiania luk wyświetli pytanie o utworzenie reguły lub zadania naprawy luki.

     Domyślnie opcja ta jest włączona.

   - **Akceptuj aktualizacje, które naprawiają tę lukę**

     Instalacja aktualizacji, które naprawiają lukę, zostanie zaakceptowana. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

     Domyślnie opcja ta jest wyłączona.
5. Jeśli wybierzesz wyszukiwanie istniejących zadań naprawiania luk i wyszukiwanie znajdzie zadania, możesz przejrzeć właściwości tych zadań lub uruchomić je ręcznie. Dalsze działania nie są wymagane.

   W przeciwnym razie kliknij przycisk **Nowe zadanie naprawiania luk**.
6. Wybierz typ reguły naprawiania luki, która ma zostać dodana do nowego zadania, a następnie kliknij przycisk **Zakończ**.
7. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania

wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

Zostanie uruchomiony kreator tworzenia zadania naprawy luk oraz instalacji aktualizacji. Postępuj zgodnie z krokami kreatora.

8. W oknie **Wybieranie sposobu ponownego uruchomienia systemu operacyjnego** wybierz działanie, jakie zostanie wykonane, gdy system operacyjny na urządzeniach klienckich musi zostać uruchomiony ponownie po działaniu:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Uruchom ponownie po (min)**

    Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

    Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

Domyślnie opcja ta jest wyłączona.

9. W oknie **Wybierz urządzenia, do których zostanie przypisane zadanie** wybierz jedną z następujących opcji:

- Wybierz urządzenia wykryte w sieci przez Serwer administracyjny

  Zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

  Na przykład, możesz chcieć użyć tej opcji w zadaniu instalowania Agenta sieciowego na nieprzypisanych urządzeniach.

- Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy

  Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

  Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- Przypisz zadanie do wyboru urządzeń

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

- Przypisz zadanie do grupy administracyjnej

  Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

10. W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- Zaplanowane uruchomienie:

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

- **Co N godzin**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

- **Co N dni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

  Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N tygodni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

  Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- **Co N minut**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

  Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po epidemii wirusa**

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- **Po zakończeniu wykonywania innego zadania**

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- **Uruchom pominięte zadania**

Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

Domyślnie opcja ta jest włączona.

- **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

11. W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

12. W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zamknąć kreator.

    Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Po zakończeniu działania kreatora, zadanie **Zainstaluj wymagane aktualizacje i napraw luki** jest tworzone i wyświetlane w folderze **Zadania**.

Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Naprawianie luk poprzez dodanie reguły do istniejącego zadania naprawiania luk

W celu naprawienia luki poprzez dodanie reguły do istniejącego zadania naprawiania luk:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.
2. Wybierz lukę, którą chcesz naprawić.
3. Kliknij przycisk **Uruchom kreatora naprawiania luk**.

   Zostanie uruchomiony Kreator naprawiania luk.

   > Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

   Postępuj zgodnie z krokami kreatora.
4. W oknie **Wyszukaj istniejące zadania naprawiania luk** określ następujące parametry:

   - **Pokaż tylko zadania naprawiające tę lukę**

     Jeśli ta opcja jest wyłączona, Kreator naprawiania luk wyszukuje istniejące zadania, które naprawiają wybraną lukę.

     Jeśli ta opcja jest wyłączona lub wyszukiwanie nie znajdzie stosowanych zadań, Kreator naprawiania luk wyświetli pytanie o utworzenie reguły lub zadania naprawy luki.

     Domyślnie opcja ta jest włączona.

   - **Akceptuj aktualizacje, które naprawiają tę lukę**

     Instalacja aktualizacji, które naprawiają lukę, zostanie zaakceptowana. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

     Domyślnie opcja ta jest wyłączona.
5. Jeśli wybierzesz wyszukiwanie istniejących zadań naprawiania luk i wyszukiwanie znajdzie zadania, możesz przejrzeć właściwości tych zadań lub uruchomić je ręcznie. Dalsze działania nie są wymagane.

   W innym przypadku kliknij przycisk **Dodaj regułę naprawiania luk do istniejącego zadania**.
6. Wybierz zadanie, do którego chcesz dodać regułę, a następnie kliknij przycisk **Dodaj regułę**.

   Możesz także przejrzeć właściwości istniejących zadań, uruchomić je ręcznie lub utworzyć nowe zadanie.
7. Wybierz typ reguły, która zostanie dodana do wybranego zadania, a następnie kliknij przycisk **Zakończ**.
8. Dokonaj wyboru w wyświetlonym oknie z pytaniem o zainstalowanie wszystkich poprzednich aktualizacji aplikacji. Kliknij **Tak**, jeśli wyrażasz zgodę na instalację kolejnych wersji aplikacji, jeśli jest to wymagane do zainstalowania wybranych aktualizacji. Kliknij **Nie**, jeśli chcesz aktualizować aplikację w sposób prosty, bez instalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

Nowa reguła naprawiania luk zostanie dodana do istniejącego zadania **Instalacja wymaganych aktualizacji i naprawa luk**.

Naprawianie luk w odizolowanej sieci

W tej sekcji opisano kroki, które możesz podjąć, aby usunąć luki w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach podłączonych do serwerów administracyjnych bez dostępu do Internetu.

Scenariusz: Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci

Możesz instalować aktualizacje i eliminować luki w oprogramowaniu innych firm zainstalowanym na zarządzanych urządzeniach w odizolowanej sieci. Takie sieci obejmują serwery administracyjne i podłączone do nich zarządzane urządzenia, które nie mają dostępu do Internetu. Aby naprawić luki w takiej sieci, potrzebujesz serwera administracyjnego połączonego z Internetem. Następnie będzie można pobierać poprawki z aktualizacjami przy użyciu serwera administracyjnego z dostępem do Internetu i przesyłać poprawki do odizolowanych serwerów administracyjnych.

Możesz pobrać aktualizacje oprogramowania innych firm wydane przez dostawców oprogramowania, ale nie możesz pobierać aktualizacji oprogramowania firmy Microsoft na odizolowanych serwerach administracyjnych przy użyciu Kaspersky Security Center.

Aby dowiedzieć się, jak działa proces naprawiania luk w odizolowanej sieci, zapoznaj się z opisem i schematem tego procesu.

Wymagania wstępne

Zanim zaczniesz, wykonaj następujące czynności:

1. Przydziel jedno urządzenie do łączenia się z internetem i pobierania poprawek. To urządzenie będzie liczone jako Serwer administracyjny z dostępem do internetu.
2. Zainstaluj Kaspersky Security Center, w wersji co najmniej 14, na następujących urządzeniach:
   - Przydzielone urządzenie, które będzie pełnić rolę serwera administracyjnego z dostępem do Internetu
   - Izolowane urządzenia, które będą działać jako izolowane od Internetu serwery administracyjne (zwane dalej odizolowanymi serwerami administracyjnymi)
3. Upewnij się, że każdy Serwer administracyjny ma: wystarczająco dużo miejsca na dysku do pobierania i przechowywania aktualizacji i poprawek.

Etapy

Instalowanie aktualizacji i eliminowanie luk w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach izolowanych serwerów administracyjnych obejmuje następujące etapy:

1. **Konfigurowanie serwera administracyjnego z dostępem do Internetu**

   Przygotuj swój Serwer administracyjny z dostępem do Internetu do obsługi żądań dotyczących wymaganych aktualizacji oprogramowania innych firm i pobierania poprawek.

2. **Konfigurowanie izolowanych Serwerów administracyjnych**

Przygotuj odizolowane serwery administracyjne, dzięki czemu mogą tworzyć listy wymaganych aktualizacji i obsługiwać poprawki pobrane przez serwer administracyjny z dostępem do Internetu. Po skonfigurowaniu odizolowane serwery administracyjne nie próbują już pobierać poprawek z Internetu. Zamiast tego uzyskują aktualizacje przez poprawki.

3. **Przesyłanie poprawek i instalowanie aktualizacji na odizolowanych serwerach administracyjnych**

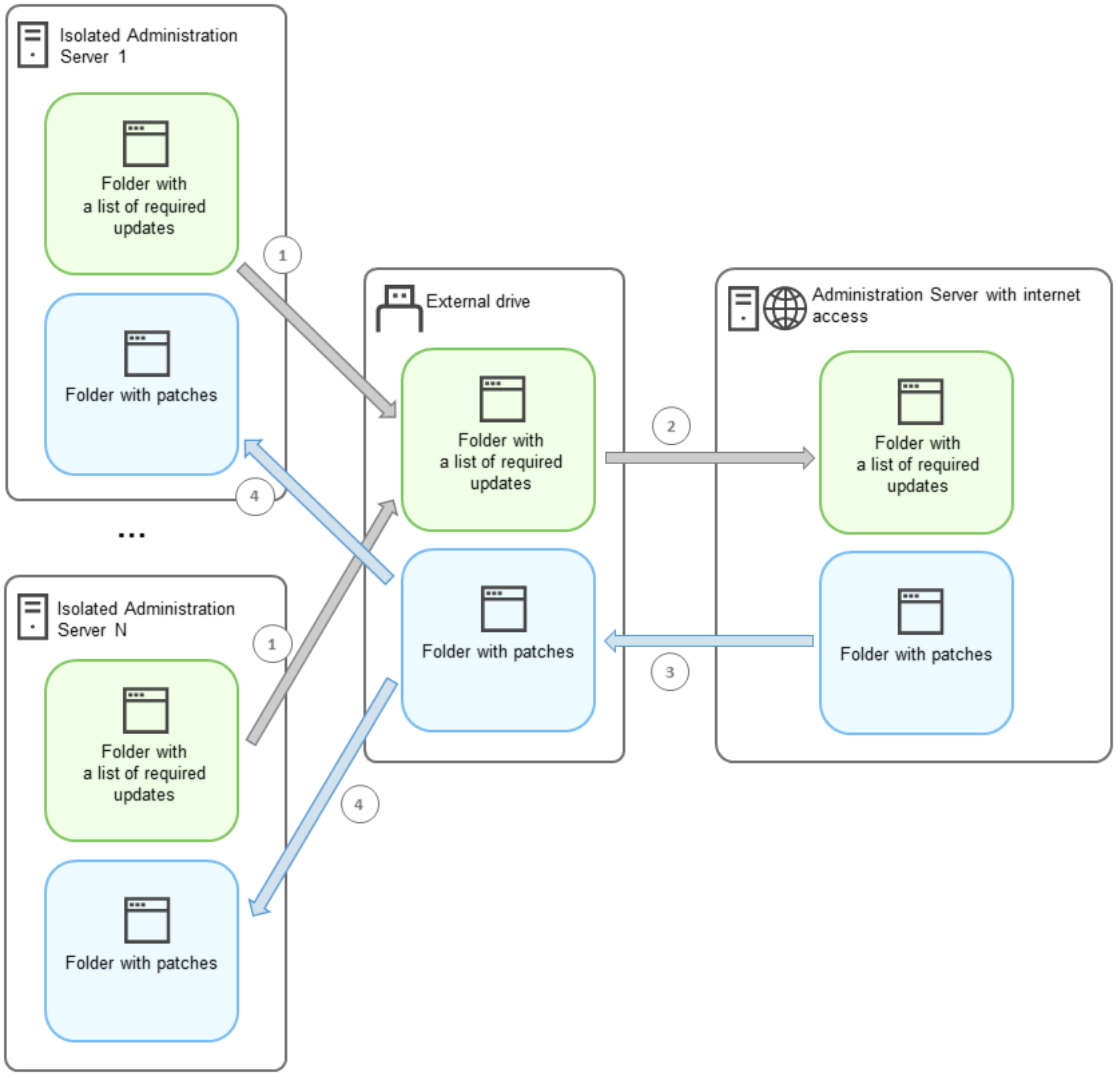
   Po zakończeniu konfigurowania serwerów administracyjnych możesz: przesyłać wymagane listy aktualizacji i poprawki pomiędzy serwerem administracyjnym z dostępem do Internetu a odizolowanymi serwerami administracyjnymi. Następnie aktualizacje z poprawek zostaną zainstalowane na zarządzanych urządzeniach przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

Wyniki

W ten sposób uaktualnienia oprogramowania firm trzecich są przesyłane do odizolowanych serwerów administracyjnych i instalowane na podłączonych zarządzanych urządzeniach za pomocą Kaspersky Security Center. Wystarczy raz skonfigurować serwery administracyjne, a potem możesz otrzymywać aktualizacje tak często, jak potrzebujesz, na przykład raz lub kilka razy dziennie.

Eliminowanie luk w oprogramowaniu innych firm w odizolowanej sieci

Proces naprawiania luk w zabezpieczeniach oprogramowania firm trzecich w odizolowanej sieci jest przedstawiony na rysunku i opisany poniżej. Możesz okresowo powtarzać ten proces.



Każdy serwer administracyjny odizolowany od Internetu (zwany dalej izolowanym serwerem administracyjnym) generuje listę aktualizacji, które należy zainstalować na zarządzanych urządzeniach podłączonych do tego serwera administracyjnego. Lista wymaganych aktualizacji jest przechowywana w określonym folderze i przedstawia zestaw plików binarnych. Każdy plik ma nazwę zawierającą identyfikator poprawki z wymaganą aktualizacją. W rezultacie każdy plik na liście wskazuje konkretną poprawkę.

Używając zewnętrznego dysku, przenosisz listę wymaganych aktualizacji z izolowanego Serwera administracyjnego na przydzielony Serwer administracyjny z dostępem do Internetu. Następnie przydzielony Serwer administracyjny pobiera poprawki z Internetu i umieszcza je w osobnym folderze.

Po pobraniu wszystkich poprawek i umieszczeniu ich w specjalnym dla nich folderze, przenosisz je na każdy odizolowany Serwer administracyjny, z którego pobrałeś listę wymaganych uaktualnień. Poprawki zapisujesz do folderu utworzonego specjalnie dla nich na izolowanym Serwerze administracyjnym. W rezultacie zadanie *Zainstaluj wymagane aktualizacje i napraw luki* uruchamia poprawki i instaluje aktualizacje na zarządzanych urządzeniach izolowanych Serwerów administracyjnych.

Konfigurowanie serwera administracyjnego z dostępem do internetu w celu usunięcia luk w odizolowanej sieci

Aby przygotować się na usuwanie luk i przesyłanie poprawek w izolowanej sieci, najpierw skonfiguruj serwer administracyjny z dostępem do Internetu, a następnie skonfiguruj odizolowane serwery administracyjne.

W celu skonfigurowania serwera administracyjnego z dostępem do Internetu:

1. Utwórz dwa foldery na dysku, na którym zainstalowany jest serwer administracyjny:

   - Folder z listą wymaganych aktualizacji
   - Folder na poprawki

   Możesz nazwać te foldery tak, jak chcesz.

2. Przyznaj prawa dostępu do modyfikacji do grupy KLAdmins w utworzonych folderach, korzystając ze standardowych narzędzi administracyjnych systemu operacyjnego.

3. Użyj narzędzia klscflag, aby zapisać ścieżki do folderów we właściwościach Serwera administracyjnego. Wpisz następujące polecenia w wierszu polecenia systemu Windows, korzystając z uprawnień administratora:

   - W celu ustawienia ścieżki do folderu dla poprawek:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<ścieżka do folderu>"`
   - W celu ustawienia ścieżki do folderu dla listy wymaganych aktualizacji:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<ścieżka do folderu>"`

   Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\FolderForPatches"`

4. [Opcjonalnie] Użyj narzędzia klscflag, aby określić, jak często Serwer administracyjny powinien sprawdzać nowe żądania poprawek:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <wartość w sekundach>`

Domyślna wartość to 120 sekund.

Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

5. Uruchom ponownie usługę Serwera administracyjnego.

Teraz serwer administracyjny z dostępem do Internetu jest gotowy do pobierania i przesyłania aktualizacji do izolowanych serwerów administracyjnych. Zanim zaczniesz naprawiać luki, skonfiguruj izolowane serwery administracyjne.

Konfigurowanie izolowanych Serwerów administracyjnych w celu usunięcia luk w odizolowanej sieci

Po zakończeniu konfigurowania serwera administracyjnego z dostępem do internetu, przygotuj każdy odizolowany serwer administracyjny w Twojej sieci, abyś mógł: wyeliminować luki i zainstalować aktualizacje na zarządzanych urządzeniach podłączonych do izolowanych serwerów administracyjnych.

Aby skonfigurować izolowane serwery administracyjne, wykonaj następujące czynności na każdym serwerze administracyjnym:

1. Aktywuj klucz licencyjny dla funkcji Zarządzanie lukami i poprawkami (VAPM).

2. Utwórz dwa foldery na dysku, na którym zainstalowany jest serwer administracyjny:

   - Folder, w którym pojawi się lista wymaganych aktualizacji
   - Folder na poprawki

   Możesz nazwać te foldery tak, jak chcesz.

3. Przyznaj *uprawnienia do modyfikacji* do grupy KLAdmins w utworzonych folderach, korzystając ze standardowych narzędzi administracyjnych systemu operacyjnego.

4. Użyj narzędzia klscflag, aby zapisać ścieżki do folderów we właściwościach Serwera administracyjnego. Wpisz następujące polecenia w wierszu polecenia systemu Windows, korzystając z uprawnień administratora:

   - W celu ustawienia ścieżki do folderu dla poprawek:
     `klshcflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<ścieżka do folderu>"`
   - W celu ustawienia ścieżki do folderu dla listy wymaganych aktualizacji:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<ścieżka do folderu>"`

   Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\FolderForPatches"`

5. [Opcjonalnie] Użyj narzędzia klscflag, aby określić, jak często izolowany serwer administracyjny powinien sprawdzać dostępność nowych poprawek:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <wartość w sekundach>`

   Domyślna wartość to 120 sekund.

   Na przykład: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

6. [Opcjonalnie] Użyj narzędzia klscflag, aby obliczyć skróty SHA-256 poprawek:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

Jeśli wprowadzisz to polecenie, możesz się upewnić, że poprawki nie zostały zmodyfikowane podczas przesyłania na izolowany Serwer administracyjny oraz że otrzymano prawidłowe poprawki zawierające wymagane aktualizacje.

Domyślnie, Kaspersky Security Center nie oblicza skrótów SHA-256 poprawek. Jeśli włączysz tę opcję, po odebraniu przez izolowany serwer administracyjny poprawek, Kaspersky Security Center oblicza ich skróty i porównuje uzyskane wartości ze skrótami przechowywanymi w bazie danych serwera administracyjnego. Jeśli obliczony skrót nie zgadza się ze skrótem w bazie danych, pojawia się błąd i trzeba zastąpić nieprawidłowe poprawki.

7. Utwórz zadanie *Wyszukiwanie luk i wymaganych aktualizacji* i ustaw harmonogram zadań. Uruchom zadanie, jeśli chcesz, aby zostało uruchomione wcześniej niż jest to określone w harmonogramie zadań.

8. Uruchom ponownie usługę Serwera administracyjnego.

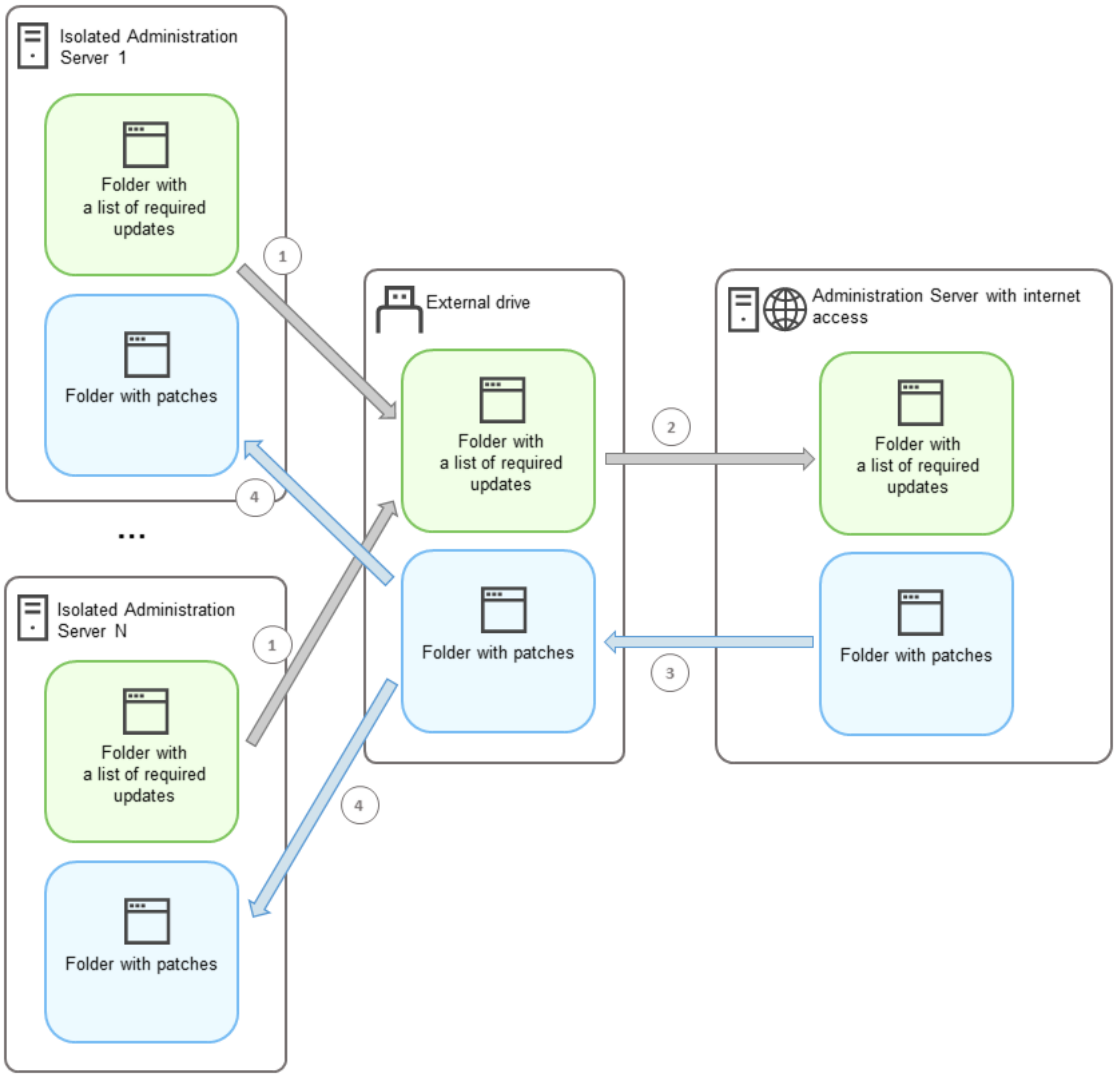
Po skonfigurowaniu wszystkich serwerów administracyjnych możesz: zarządzać poprawkami i listami wymaganych aktualizacji oraz eliminować luki w zabezpieczeniach oprogramowania firm trzecich na zarządzanych urządzeniach w odizolowanej sieci.

Przesyłanie poprawek i instalowanie aktualizacji w odizolowanej sieci

Po zakończeniu konfigurowania serwerów administracyjnych możesz przesyłać poprawki zawierające wymagane aktualizacje z serwera administracyjnego z dostępem do Internetu na izolowane serwery administracyjne. Możesz przesyłać i instalować aktualizacje tak często, jak potrzebujesz, na przykład, raz lub kilka razy dziennie.

Do przesyłania poprawek i listy wymaganych uaktualnień między Serwerami administracyjnymi potrzebny jest dysk zewnętrzny. Dlatego upewnij się, że na dysku zewnętrznym jest wystarczająco dużo miejsca do pobierania i przechowywania poprawek.

Proces przesyłania poprawek oraz lista wymaganych aktualizacji są wyświetlane na rysunku i opisane poniżej:



Proces przesyłania poprawek i lista wymaganych aktualizacji między serwerem administracyjnym z dostępem do Internetu a izolowanymi serwerami administracyjnymi

W celu zainstalowania aktualizacji i usunięcia luk na zarządzanych urządzeniach podłączonych do izolowanych Serwerów administracyjnych:

1. Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, jeśli nie zostało jeszcze uruchomione.
2. Podłącz dysk zewnętrzny do dowolnego izolowanego Serwera administracyjnego.
3. Utwórz dwa foldery na dysku zewnętrznym: jeden na listę wymaganych aktualizacji, a drugi na poprawki. Możesz nazwać te foldery tak, jak chcesz.

   Jeśli wcześniej utworzono foldery, wyczyść je.
4. Skopiuj listę wymaganych aktualizacji z każdego izolowanego Serwera administracyjnego i wklej tę listę do folderu z listą wymaganych aktualizacji na dysku zewnętrznym.

   W rezultacie wszystkie listy uzyskane ze wszystkich izolowanych serwerów administracyjnych łączysz w jeden folder. Folder ten powinien zawierać pliki binarne z identyfikatorami poprawek wymaganych dla wszystkich izolowanych serwerów administracyjnych.
5. Podłącz dysk zewnętrzny do Serwera administracyjnego z dostępem do Internetu.
6. Skopiuj listę wymaganych aktualizacji z dysku zewnętrznego i wklej tę listę do folderu listy wymaganych aktualizacji na Serwerze administracyjnym z dostępem do Internetu.

Wszystkie wymagane poprawki są automatycznie pobierane z Internetu do folderu łatek na Serwerze administracyjnym. To może potrwać kilka godzin.

7. Upewnij się, że wszystkie wymagane poprawki zostały pobrane. W tym celu możesz wykonać jedną z następujących czynności:

   - Sprawdź folder w poszukiwaniu poprawek na Serwerze administracyjnym z dostępem do internetu. Wszystkie poprawki, które zostały określone na liście wymaganych aktualizacji, należy pobrać do odpowiedniego folderu. Jest to wygodniejsze, jeśli wymagana jest niewielka liczba poprawek.

   - Przygotuj specjalny skrypt, na przykład, skrypt powłoki. Jeśli otrzymasz dużą liczbę poprawek, trudno będzie samodzielnie sprawdzić, czy wszystkie poprawki zostały pobrane. W takich przypadkach lepiej zautomatyzować sprawdzanie.

8. Skopiuj poprawki z Serwera administracyjnego z dostępem do Internetu i wklej je do odpowiedniego folderu na dysku zewnętrznym.

9. Prześlij poprawki do każdego izolowanego Serwera administracyjnego. Umieść poprawki w specjalnym folderze.

W rezultacie każdy izolowany serwer administracyjny tworzy aktualną listę aktualizacji i poprawek wymaganych dla zarządzanych urządzeń podłączonych do bieżącego serwera administracyjnego. Po otrzymaniu przez serwer administracyjny z dostępem do Internetu listy wymaganych aktualizacji, serwer administracyjny pobiera poprawki z aktualizacjami z Internetu. Gdy te poprawki pojawią się na odizolowanych serwerach administracyjnych, zadanie *Zainstaluj wymagane aktualizacje i napraw luki* obsługuje poprawki. Aktualizacje są instalowane na zarządzanych urządzeniach, a luki w zabezpieczeniach oprogramowania innych firm są naprawiane.

Gdy uruchomione jest zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, nie uruchamiaj ponownie urządzenia serwera administracyjnego ani nie uruchamiaj zadania *Kopia zapasowa danych Serwera administracyjnego* (spowoduje to również ponowne uruchomienie). W rezultacie zadanie *Zainstaluj wymagane aktualizacje i napraw luki* zostanie przerwane, a aktualizacje nie zostaną zainstalowane. W takim przypadku musisz zrestartować to zadanie ręcznie lub poczekać na uruchomienie zadania zgodnie ze skonfigurowanym harmonogramem.

Wyłączanie możliwości przesyłania poprawek i instalowania aktualizacji w odizolowanej sieci

Można wyłączyć przesyłanie poprawek na izolowanych serwerach administracyjnych, na przykład, jeśli zdecydowano się usunąć jeden lub więcej serwerów z odizolowanej sieci. W ten sposób możesz zmniejszyć liczbę poprawek i czas ich pobierania.

W celu wyłączenia możliwości przekazania poprawek na izolowanych serwerach administracyjnych:

1. Jeśli chcesz wyizolować wszystkie serwery administracyjne, we właściwościach serwera administracyjnego z dostępem do Internetu usuń ścieżki do folderów z poprawkami oraz listę wymaganych aktualizacji. Jeśli chcesz, aby niektóre serwery administracyjne znajdowały się w odizolowanej sieci, pomiń ten krok.

   Wpisz następujące polecenia w wierszu polecenia systemu Windows, korzystając z uprawnień administratora:

   - W celu usunięcia ścieżki do folderu dla poprawek:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```

   - W celu usunięcia ścieżki do folderu dla listy wymaganych aktualizacji:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Uruchom ponownie usługę serwera administracyjnego, jeśli usunięto ścieżki do folderów na tym serwerze administracyjnym.

3. We właściwościach każdego serwera administracyjnego, który chcesz wyłączyć z izolacji, usuń ścieżki do folderów z poprawkami oraz listę wymaganych aktualizacji.

   Wpisz następujące polecenia w wierszu polecenia systemu Windows, korzystając z uprawnień administratora:

   - W celu usunięcia ścieżki do folderu dla poprawek:
     ```
     klshcflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - W celu usunięcia ścieżki do folderu dla listy wymaganych aktualizacji:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Uruchom ponownie każdy serwer administracyjny, z którego usunięto ścieżki do folderów.

W rezultacie, jeśli zmieniono konfigurację serwera administracyjnego z dostępem do Internetu, nie będziesz już otrzymywać poprawek za pośrednictwem Kaspersky Security Center. Jeżeli zmieniono konfigurację tylko niektórych odizolowanych serwerów administracyjnych, np. usuwając niektóre z nich z izolowanej sieci, otrzymasz poprawki tylko dla pozostałych izolowanych serwerów administracyjnych.

Jeśli chcesz w przyszłości rozpocząć eliminowanie luk w zabezpieczeniach na wyłączonych izolowanych serwerach administracyjnych, musisz skonfigurować te serwery i serwer z dostępem do Internetu jeszcze raz.

Ignorowanie luk w oprogramowaniu

Możesz zignorować luki w oprogramowaniu, które mają zostać naprawione. Przyczyny zignorowania luk w oprogramowaniu mogą być, na przykład, następujące:

- Nie uważasz luki w oprogramowaniu za krytyczną dla swojej organizacji.
- Rozumiesz, poprawka luki w oprogramowaniu może uszkodzić dane związane z oprogramowaniem, które wymagało naprawy luki.
- Jesteś pewien, że luka w oprogramowaniu nie jest niebezpieczna dla sieci w Twojej organizacji, ponieważ używasz innych środków ochrony swoich zarządzanych urządzeń.

Możesz zignorować lukę w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wszystkich zarządzanych urządzeniach:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

   Obszar roboczy folderu wyświetla listę luk w aplikacjach, wykrytych na urządzeniach przez zainstalowanego na nich Agenta sieciowego.

2. Wybierz lukę, którą chcesz zignorować.

3. Z menu kontekstowego luki wybierz **Właściwości**.

   Zostanie otwarte okno właściwości luki.

4. W sekcji **Ogólny** wybierz opcję **Ignoruj lukę**.

5. Kliknij **OK**.

   Okno właściwości luki w oprogramowaniu zostanie zamknięte.

Luka w oprogramowaniu zostanie zignorowana na wszystkich zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wybranym zarządzanym urządzeniu:

1. Otwórz okno właściwości wybranego zarządzanego urządzenia i wybierz sekcję **Luki w oprogramowaniu**.
2. Wybierz lukę w oprogramowaniu.
3. Zignoruj wybraną lukę.

Luka w oprogramowaniu zostanie zignorowana na wybranym urządzeniu.

Zignorowana luka w oprogramowaniu nie zostanie naprawiona po zakończeniu wykonywania zadania *Napraw luki* lub zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Możesz wykluczyć zignorowane luki w oprogramowaniu z listy luk, korzystając z filtra.

Wybieranie poprawek użytkownika dla luk w programach innych firm

Aby użyć zadania *Napraw luki*, należy ręcznie określić aktualizacje oprogramowania do naprawy luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm. *Poprawki użytkownika* to aktualizacje oprogramowania do naprawy luk, które administrator ręcznie określa do zainstalowania.

W celu wybrania poprawek użytkownika dla luk w programach firm trzecich:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Luki w oprogramowaniu**.

   Obszar roboczy folderu wyświetla listę luk w aplikacjach, wykrytych na urządzeniach przez zainstalowanego na nich Agenta sieciowego.

2. Wybierz lukę, dla której chcesz określić poprawkę użytkownika.
3. Z menu kontekstowego luki wybierz **Właściwości**.

   Zostanie otwarte okno właściwości luki.

4. W sekcji **Poprawki użytkownika i inne poprawki** kliknij przycisk **Dodaj**.

   Zostanie wyświetlona lista dostępnych pakietów instalacyjnych. Lista wyświetlonych pakietów instalacyjnych odpowiada liście **Zdalna instalacja** → **Pakiety instalacyjne**. Jeśli nie utworzono pakietu instalacyjnego zawierającego poprawkę użytkownika dla wybranej luki, możesz utworzyć pakiet teraz, uruchamiając Kreator tworzenia nowego pakietu.

5. Wybierz pakiet (lub pakiety) instalacyjny zawierający poprawkę użytkownika (lub poprawki użytkownika) dla luki w oprogramowaniu innych firm.
6. Kliknij **OK**.

Zostaną określone pakiety instalacyjne zawierające poprawki użytkownika dla luki w oprogramowaniu. Jeśli zadanie jest uruchamiane *Napraw luki*, pakiet instalacyjny zostanie zainstalowany, a luka w oprogramowaniu zostanie wyeliminowana.

Reguły instalacji aktualizacji

Jeśli usuwasz luki w aplikacjach, musisz określić reguły instalacji aktualizacji. Te reguły określają aktualizacje do zainstalowania oraz luki do wyeliminowania.

Dokładne ustawienia zależą od tego, czy tworzysz regułę dla aktualizacji aplikacji firmy Microsoft, aplikacji firm trzecich (aplikacje stworzone przez producentów oprogramowania innych niż Kaspersky i Microsoft) lub wszystkich aplikacji. Podczas tworzenia reguł dla aplikacji firmy Microsoft lub aplikacji firm trzecich możesz wybrać określone aplikacje oraz wersje aplikacji, dla których chcesz zainstalować uaktualnienia. Podczas tworzenia reguły dla wszystkich aplikacji możesz wybrać określone uaktualnienia, które chcesz zainstalować, oraz luki, które chcesz wyeliminować poprzez zainstalowanie uaktualnień.

W celu utworzenia reguły dla uaktualnień wszystkich aplikacji:

1. Na stronie **Ustawienia** kreatora tworzenia nowego zadania kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Postępuj zgodnie z krokami kreatora.

2. W kroku **Typ reguły** wybierz **Reguła dla wszystkich aktualizacji**.

3. W kroku **Kryteria ogólne** użyj list rozwijalnych do określenia następujących ustawień:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aktualizacje** wybierz aktualizacje, które mają zostać zainstalowane:

   - **Zainstaluj wszystkie pasujące aktualizacje**

Zainstaluj aktualizacje oprogramowania, które spełniają kryteria określone w kroku **Kryteria ogólne**. Ta opcja jest wybrana domyślnie.

- **Zainstaluj tylko aktualizacje z listy**

  Instalowane są tylko te aktualizacje oprogramowania, które wybierzesz ręcznie z listy. Ta lista zawiera wszystkie dostępne aktualizacje oprogramowania.

  Na przykład, możesz wybrać określone aktualizacje w następujących przypadkach: aby sprawdzić ich instalację w środowisku testowym, aby zaktualizować tylko krytyczne aplikacje lub aby zaktualizować tylko określone aplikacje.

  - **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

    Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

    Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

    Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

    Domyślnie opcja ta jest włączona.

5. W kroku **Luki** wybierz luki, które zostaną wyeliminowane poprzez zainstalowanie wybranych aktualizacji:

   - **Napraw wszystkie luki spełniające inne kryteria**

     Wyeliminuj wszystkie luki, które spełniają kryteria określone na stronie **Kryteria ogólne** kreatora. Ta opcja jest wybrana domyślnie.

   - **Napraw tylko luki z listy**

     Naprawione zostaną tylko te luki, które ręcznie wybierzesz z listy. Ta lista zawiera wszystkie wykryte luki.

     Na przykład, możesz wybrać określone luki w następujących przypadkach: aby sprawdzić ich eliminację w środowisku testowym, aby wyeliminować luki tylko w krytycznych aplikacjach lub aby wyeliminować luki tylko w określonych aplikacjach.

6. W kroku **Nazwa** określ nazwę dla reguły, którą tworzysz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie utworzona i wyświetlona w polu **Określ reguły instalacji aktualizacji** Kreatora tworzenia nowego zadania.

W celu utworzenia reguły dla aktualizacji aplikacji firmy Microsoft:

1. Na stronie **Ustawienia** kreatora tworzenia nowego zadania kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Postępuj zgodnie z krokami kreatora.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji systemu Windows**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

   - **Napraw luki z priorytetem MSRC równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni, Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Kategorie aktualizacji** wybierz kategorie aktualizacji, które mają zostać zainstalowane. Te kategorie są takie same, jak w Microsoft Update Catalog. Domyślnie, zaznaczone są wszystkie kategorie.

6. W kroku **Nazwa** określ nazwę dla reguły, którą tworzysz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora, nowa reguła zostanie utworzona i wyświetlona w polu **Określ reguły instalacji aktualizacji** Kreator tworzenia nowego zadania.

W celu utworzenia nowej reguły dla aktualizacji aplikacji firm trzecich:

1. Na stronie **Ustawienia** kreatora tworzenia nowego zadania kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Postępuj zgodnie z krokami kreatora.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji firm trzecich**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - Zbiór uaktualnień do zainstalowania

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - Napraw luki z priorytetem równym lub większym niż

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Nazwa** określ nazwę dla reguły, którą tworzysz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora, nowa reguła zostanie utworzona i wyświetlona w polu **Określ reguły instalacji aktualizacji** Kreator tworzenia nowego zadania.

Grupy aplikacji

Sekcja ta opisuje sposób zarządzania grupami aplikacji zainstalowanych na urządzeniach.

Tworzenie kategorii aplikacji

Kaspersky Security Center pozwala na tworzenie kategorii aplikacji zainstalowanych na urządzeniach.

Kategorie aplikacji można utworzyć w jeden z następujących sposobów:

- Administrator określa folder, z którego pliki wykonywalne zostały uwzględnione w wybranej kategorii.
- Administrator określa urządzenie, z którego pliki wykonywalne mają zostać uwzględnione w wybranej kategorii.
- Administrator ustawia kryteria, które zostaną użyte przy dodawaniu aplikacji do wybranej kategorii.

Po utworzeniu kategorii aplikacji, administrator może ustawić reguły dla tej kategorii. Reguły określają zachowanie aplikacji znajdującej się w danej kategorii. Na przykład, możesz zablokować lub zezwolić na uruchamianie aplikacji znajdujących się w kategorii.

Zarządzanie aplikacjami uruchomionymi na urządzeniach

Kaspersky Security Center umożliwia zarządzanie uruchamianiem aplikacji na urządzeniach w trybie Biała lista. Więcej informacji można znaleźć w internetowym systemie pomocy dla Kaspersky Endpoint Security for Windows. W trakcie pracy w trybie Biała lista, na wybranych urządzeniach możesz uruchamiać aplikacje tylko z określonych kategorii. Administrator może wyświetlić wyniki analizy statystycznej zastosowanej na regułach uruchamiania aplikacji na urządzeniach dla każdego użytkownika.

Inwentaryzacja oprogramowania zainstalowanego na urządzeniach

Kaspersky Security Center pozwala na przeprowadzanie inwentaryzacji oprogramowania na urządzeniach działających pod kontrolą systemu Windows. Agent sieciowy pobiera informacje o wszystkich aplikacjach zainstalowanych na urządzeniach. Informacje zebrane w trakcie inwentaryzacji są wyświetlane w obszarze roboczym folderu **Rejestr aplikacji**. Administrator może wyświetlić szczegółowe informacje o każdej aplikacji, łącznie z wersją i producentem.

Liczba plików wykonywalnych pobranych z jednego urządzenia nie może przekraczać 150 000. Po osiągnięciu tego limitu, Kaspersky Security Center nie będzie mógł otrzymywać nowych plików.

Zarządzanie grupą licencjonowanych aplikacji

Kaspersky Security Center pozwala na tworzenie grup licencjonowanych aplikacji. Grupa licencjonowanych aplikacji zawiera aplikacje spełniające kryteria ustalone przez administratora. Administrator może określić następujące kryteria dla grup licencjonowanych aplikacji:

- Nazwa aplikacji
- Wersja aplikacji
- Producent
- Znacznik aplikacji

Aplikacje spełniające jedno lub kilka kryteriów są automatycznie dodawane do grupy. Aby utworzyć grupę licencjonowanych aplikacji, musisz ustawić przynajmniej jedno kryterium dodawania aplikacji do takiej grupy.

Każda grupa licencjonowanych aplikacji posiada swój klucz licencyjny. Klucz licencyjny grupy licencjonowanych aplikacji określa maksymalną dozwoloną liczbę instalacji aplikacji wchodzących w skład tej grupy. Jeśli liczba instalacji przekroczyła ograniczenie ustawione przez klucz licencyjny, na Serwerze administracyjnym zostanie zarejestrowane zdarzenie informacyjne. Administrator może określić datę wygaśnięcia dla klucza licencyjnego. Po nadejściu tej daty, na Serwerze administracyjnym jest zapisywane zdarzenie informacyjne.

Przeglądanie informacji o plikach wykonywalnych

Kaspersky Security Center pobiera wszystkie informacje o plikach wykonywalnych, które były uruchamiane na urządzeniach od momentu zainstalowania na nich systemu operacyjnego. Zebrane informacje o plikach wykonywalnych są wyświetlane w oknie głównym aplikacji, w obszarze roboczym folderu **Pliki wykonywalne**.

Scenariusz: Zarządzanie aplikacjami

Możesz zarządzać uruchamianiem aplikacji na urządzeniach użytkowników. Możesz zezwolić na lub zablokować uruchamianie aplikacji na zarządzanych urządzeniach. Ta funkcjonalność jest realizowana przez komponent Kontrola aplikacji. Możesz zarządzać aplikacjami zainstalowanymi na urządzeniach z systemem Windows lub Linux.

W przypadku systemów operacyjnych opartych na systemie Linux komponent Kontrola aplikacji jest dostępny począwszy od Kaspersky Endpoint Security 11.2 for Linux.

Wymagania wstępne

- Kaspersky Security Center zostanie wdrożony w Twojej organizacji.
- Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Linux został utworzony i jest aktywny.

Etapy

Scenariusz korzystania z Kontroli aplikacji podzielony jest na etapy:

1. **Tworzenie i przeglądanie listy aplikacji na urządzeniach klienckich**

   Ten etap pomaga w odnalezieniu aplikacji, które są zainstalowane na zarządzanych urządzeniach. Możesz przejrzeć listę aplikacji i zdecydować, na które aplikacje chcesz zezwolić, a które chcesz zablokować zgodnie z polityką bezpieczeństwa organizacji. Ograniczenia mogą dotyczyć polityki bezpieczeństwa informacji, obowiązującej w Twojej organizacji. Możesz pominąć ten etap, jeśli wiesz dokładnie, jakie aplikacje są zainstalowane na zarządzanych urządzeniach.

   Dostępne instrukcje:

   - Konsola administracyjna: Przeglądanie rejestru aplikacji
   - Kaspersky Security Center Web Console: Uzyskiwanie i przeglądanie listy aplikacji zainstalowanych na urządzeniach klienckich

2. **Tworzenie i przeglądanie listy plików wykonywalnych na urządzeniach klienckich**

Ten etap pomaga w odnalezieniu plików wykonywalnych, które znajdują się na zarządzanych urządzeniach. Przejrzyj listę plików wykonywalnych i porównaj ją z listami dozwolonych i zabronionych plików wykonywalnych. Ograniczenia dotyczące użycia plików wykonywalnych mogą być związane z polityką bezpieczeństwa informacji, obowiązującej w Twojej organizacji. Możesz pominąć ten etap, jeśli wiesz dokładnie, jakie pliki wykonywalne są zainstalowane na zarządzanych urządzeniach.

Dostępne instrukcje:

- Konsola administracyjna: Inwentaryzacja plików wykonywalnych
- Kaspersky Security Center Web Console: Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

3. **Tworzenie kategorii aplikacji dla aplikacji używanych w Twojej organizacji**

Przeanalizuj listy aplikacji i plików wykonywalnych, przechowywanych na zarządzanych urządzeniach. W oparciu o analizę, utwórz kategorie aplikacji. Zalecane jest utworzenie kategorii „Aplikacje do pracy", która obejmuje standardowy zestaw aplikacji używanych w Twojej organizacji. Jeśli różne grupy użytkowników używają różnych zestawów aplikacji w swojej pracy, oddzielna kategoria aplikacji może zostać utworzona dla każdej grupy użytkowników.

W zależności od zestawu kryteriów do utworzenia kategorii aplikacji możesz utworzyć kategorie aplikacji trzech typów.

Dostępne instrukcje:

- Konsola administracyjna: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranych urządzeń, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranego folderu.
- Kaspersky Security Center Web Console: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranych urządzeń, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranego folderu.

4. **Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security**

Skonfiguruj komponent Kontrola aplikacji w zasadzie Kaspersky Endpoint Security, korzystając z kategorii aplikacji, które utworzono w poprzednim kroku.

Dostępne instrukcje:

- Konsola administracyjna: Konfigurowanie zarządzania uruchamianiem aplikacji na urządzeniach klienckich
- Kaspersky Security Center Web Console: Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows

5. **Włączanie komponentu Kontrola aplikacji w trybie testowym**

Aby zapewnić, że reguły Kontroli aplikacji nie będą blokowały aplikacji wymaganych do pracy użytkownika, zalecane jest włączenie testowania reguł Kontroli aplikacji i analizowanie ich działania po utworzeniu nowych reguł. Po włączeniu testowania, Kaspersky Endpoint Security for Windows nie zablokuje aplikacji, których uruchamianie jest zablokowane przez reguły Kontroli aplikacji, ale zamiast tego wyśle powiadomienia o ich uruchomieniu do Serwera administracyjnego.

Podczas testowania reguł Kontroli aplikacji zalecane jest wykonanie następujących działań:

- Określenie okresu testowania. Okres testowania może wahać się od siedmiu dni do dwóch miesięcy.
- Sprawdź zdarzenia wynikające z testowania działania Kontroli aplikacji.

Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i włącz opcję **Tryb testowy** w procesie konfiguracji.

6. **Zmienianie ustawień kategorii aplikacji komponentu Kontrola aplikacji**

   Jeśli to konieczne, wprowadź zmiany w ustawieniach Kontroli aplikacji. W oparciu o wyniki testu, możesz dodać pliki wykonywalne związane ze zdarzeniami komponentu Kontrola aplikacji do kategorii aplikacji z zawartością dodaną ręcznie.

   Dostępne instrukcje:

   - Konsola administracyjna: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji
   - Kaspersky Security Center Web Console: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

7. **Stosowanie reguł Kontroli aplikacji w trybie działania**

   Po przetestowaniu reguł Kontroli aplikacji i zakończeniu konfiguracji kategorii aplikacji możesz zastosować reguły Kontroli aplikacji w trybie działania.

   Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i wyłącz opcję **Tryb testowy** w procesie konfiguracji.

8. **Weryfikowanie konfiguracji Kontroli aplikacji**

   Upewnij się, że wykonałeś następujące czynności:

   - Utworzyłeś kategorie aplikacji.
   - Skonfigurowałeś Kontrolę aplikacji przy użyciu kategorii aplikacji.
   - Zastosowałeś reguły Kontroli aplikacji w trybie działania.

Wyniki

Po zakończeniu scenariusza uruchamianie aplikacji na zarządzanych urządzeniach jest kontrolowane. Użytkownicy mogą uruchamiać tylko te aplikacje, które są dozwolone w Twojej organizacji, a nie mogą uruchamiać aplikacji, które są zabronione w Twojej organizacji.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Tworzenie kategorii aplikacji dla zasad Kaspersky Endpoint Security for Windows

Możesz utworzyć kategorie aplikacji dla profili Kaspersky Endpoint Security for Windows z folderu **Kategorie aplikacji** i z okna **Właściwości** profilu Kaspersky Endpoint Security for Windows.

*W celu utworzenia kategorii aplikacji dla profilu Kaspersky Endpoint Security z folderu **Kategorie aplikacji**:*

1. W drzewie konsoli wybierz **Zaawansowane** → **Zarządzanie aplikacjami** → **Kategorie aplikacji**.

2. W obszarze roboczym folderu **Kategorie aplikacji** kliknij przycisk **Nowa kategoria**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii.

3. W oknie **Typ kategorii** wybierz typ kategorii użytkownika:

   - **Ręcznie dodana kategoria z zawartością**. Określ kryteria, które będą używane do przypisywania plików wykonywalnych do tworzonej kategorii.
   - **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń**. Określ urządzenie, którego pliki wykonywalne muszą być automatycznie przypisane do tej kategorii.
   - **Kategoria zawierająca pliki wykonywalne z konkretnego folderu**. Określ folder, którego pliki wykonywalne muszą być automatycznie przypisane do tej kategorii.

4. Postępuj zgodnie z instrukcjami Kreatora.

Jeśli kreator zakończy działanie, zostanie utworzona niestandardowa kategoria aplikacji. Nowo utworzone kategorie można przeglądać, korzystając z listy kategorii w obszarze roboczym folderu **Kategorie aplikacji**.

Możesz także utworzyć kategorię aplikacji z poziomu folderu **Profile**.

*W celu utworzenia kategorii aplikacji z poziomu okna **Właściwości** profilu Kaspersky Endpoint Security for Windows:*

1. Z drzewa konsoli wybierz folder **Zasady**.

2. W obszarze roboczym folderu **Zasady** wybierz profil Kaspersky Endpoint Security, dla którego chcesz utworzyć kategorię.

3. Kliknij go prawym klawiszem myszy i wybierz **Właściwości**.

4. W oknie **Właściwości**, które zostanie otwarte, w lewym panelu **Sekcje** wybierz **Kontrola zabezpieczeń → Kontrola aplikacji**.

5. W sekcji **Kontrola aplikacji**, na listach rozwijalnych **Tryb kontroli** i **Akcja** dokonaj wyboru dla listy dozwolonych i listy blokowanych, a następnie kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Reguła Kontroli aplikacji** zawierające listę kategorii.

6. Kliknij przycisk **Utwórz nową**.

7. Wprowadź nazwę nowej kategorii i kliknij **OK**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii.

8. W oknie **Typ kategorii** wybierz typ kategorii użytkownika:

   - **Ręcznie dodana kategoria z zawartością**. Określ kryteria, które będą używane do przypisywania plików wykonywalnych do tworzonej kategorii.
   - **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń**. Określ urządzenie, którego pliki wykonywalne muszą być automatycznie przypisane do tej kategorii.
   - **Kategoria zawierająca pliki wykonywalne z konkretnego folderu**. Określ folder, którego pliki wykonywalne muszą być automatycznie przypisane do tej kategorii.

9. Postępuj zgodnie z instrukcjami Kreatora.

Jeśli kreator zakończy działanie, zostanie utworzona niestandardowa kategoria aplikacji. Możesz przeglądać nowo utworzone kategorie na liście kategorii.

Kategorie aplikacji są używane przez komponent Kontrola aplikacji znajdujący się w Kaspersky Endpoint Security for Windows. Kontrola aplikacji umożliwia administratorowi nałożenie ograniczeń na uruchamianie aplikacji na urządzeniach klienckich—na przykład, ograniczając uruchamianie aplikacji z określonej kategorii.

Tworzenie kategorii aplikacji z zawartością dodaną ręcznie

Możesz określić zestaw kryteriów jako szablon plików wykonywalnych, dla których chcesz zezwolić na lub zablokować uruchamianie w Twojej organizacji. W oparciu o pliki wykonywalne odpowiadające kryteriom, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji z zawartością dodaną ręcznie:

1. W drzewie konsoli, w folderze **Zaawansowane** → **Zarządzanie aplikacjami** wybierz podfolder **Kategorie aplikacji**.
2. Kliknij przycisk **Nowa kategoria**.

   Zostanie uruchomiony **Kreator tworzenia nowej kategorii**. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Na stronie kreatora **Typ kategorii** wybierz opcję **Kategoria z zawartością dodaną ręcznie jako typ kategorii użytkownika**.
4. Na stronie kreatora **Wprowadź nazwę kategorii aplikacji** wprowadź nową nazwę kategorii aplikacji.
5. W kroku **Konfiguracja warunków włączania aplikacji do kategorii** conditions for inclusion of applications in categories kliknij przycisk **Dodaj**.
6. Na liście rozwijalnej określ odpowiednie ustawienia:

   - **Z listy plików wykonywalnych**

     Jeśli ta opcja jest zaznaczona, możesz wskazać na liście plików wykonywalnych na urządzeniu klienckim te aplikacje, które chcesz dodać do kategorii.

   - **Z właściwości pliku**

     Jeżeli ta opcja jest zaznaczona, możesz określić szczegółowe dane dla plików wykonywalnych, które zostaną dodane do kategorii użytkownika dla aplikacji.

   - **Metadane z plików w folderze**

     Określ folder na urządzeniu klienckim, w którym znajdują się pliki wykonywalne. Metadane w plikach wykonywalnych, które znajdują się w określonym folderze, zostaną wysłane do Serwera administracyjnego. Pliki wykonywalne, które zawierają te same metadane, zostaną dodane do kategorii użytkownika.

   - **Sumy kontrolne plików znajdujących się w folderze**

Jeżeli ta opcja jest zaznaczona, możesz wybrać lub utworzyć folder na urządzeniu klienckim. Suma kontrola MD5 plików, które znajdują się w określonym folderze, zostanie wysłana do Serwera administracyjnego. Aplikacje, które mają tę samą sumę kontrolną co pliki w określonym folderze, zostaną dodane do kategorii aplikacji użytkownika.

- Certyfikaty dla plików z folderu

  Jeżeli ta opcja jest zaznaczona, możesz wskazać folder na urządzeniu klienckim, który zawiera pliki wykonywalne podpisane przez certyfikat. Certyfikaty plików wykonywalnych są do odczytu i zostają dodane do warunków kategorii. Pliki wykonywalne, które zostały podpisane zgodnie z określonymi certyfikatami, zostaną dodane do kategorii użytkownika.

- Metadane plików instalatora MSI

  Jeśli ta opcja jest zaznaczona, możesz określić plik instalatora MSI jako warunek dodania aplikacji do kategorii użytkownika. Metadane instalatora aplikacji zostaną przesłane do Serwera administracyjnego. Aplikacje, dla których metadane instalatora są takie same jak dla określonego instalatora MSI, zostaną dodane do kategorii użytkownika dla aplikacji.

- Sumy kontrolne plików z instalatora MSI aplikacji

  Jeśli ta opcja jest zaznaczona, możesz określić plik instalatora MSI jako warunek dodania aplikacji do kategorii użytkownika. Suma kontrolna plików instalatora aplikacji zostanie przesłana do Serwera administracyjnego. Aplikacje, dla których suma kontrolna pliku instalatora MSI jest taka sama, jak określona suma kontrolna, zostają dodane do kategorii aplikacji użytkownika.

- Z kategorii KL

  Jeśli ta opcja jest zaznaczona, możesz określić kategorię aplikacji Kaspersky jako warunek dodania aplikacji do kategorii użytkownika. Aplikacje z określonej kategorii Kaspersky zostaną dodane do kategorii użytkownika dla aplikacji.

- Określ ścieżkę do aplikacji (maski są obsługiwane)

  Jeżeli ta opcja zostanie zaznaczona, możesz określić ścieżkę do folderu na urządzeniu klienckim zawierający pliki wykonywalne, które zostaną dodane do kategorii użytkownika dla aplikacji.

- Wybierz certyfikat z repozytorium

  Jeśli ta opcja jest zaznaczona, możesz określić certyfikaty z repozytorium. Pliki wykonywalne, które zostały podpisane zgodnie z określonymi certyfikatami, zostaną dodane do kategorii użytkownika.

- Typ dysku

  Jeżeli ta opcja jest zaznaczona, możesz określić typ nośnika (dowolne urządzenie lub urządzenie przenośne), na którym aplikacja jest uruchomiona. Aplikacje, które były uruchomione na wybranym typie urządzenia, zostaną dodane do kategorii użytkownika dla aplikacji.

7. Na stronie kreatora **Tworzenie kategorii aplikacji** kliknij przycisk **Zakończ**.

Kaspersky Security Center zarządza tylko metadanymi z cyfrowo podpisanych plików. Nie można utworzyć kategorii w oparciu o metadane z plików, które nie zawierają podpisu cyfrowego.

Po zakończeniu działania kreatora, zostanie utworzona kategoria aplikacji użytkownika z zawartością dodaną ręcznie. Nowo utworzoną kategorię można przejrzeć, korzystając z list kategorii w obszarze roboczym folderu **Kategorie aplikacji**.

Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń

Możesz użyć plików wykonywalnych z wybranych urządzeń jako szablonu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić. W oparciu o pliki wykonywalne z wybranych urządzeń, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń:

1. W drzewie konsoli, w folderze **Zaawansowane** → **Zarządzanie aplikacjami** wybierz podfolder **Kategorie aplikacji**.

2. Kliknij przycisk **Nowa kategoria**.

   Zostanie uruchomiony **Kreator tworzenia nowej kategorii**. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Na stronie kreatora **Typ kategorii** wybierz **kategorię, która zawiera pliki wykonywalne z wybranych urządzeń** jako typ kategorii użytkownika.

4. Na stronie kreatora **Wprowadź nazwę kategorii aplikacji** wprowadź nową nazwę kategorii aplikacji.

5. Na stronie kreatora **Ustawienia** kliknij przycisk **Dodaj**.

6. Wybierz urządzenie lub urządzenia, których pliki wykonywalne zostaną użyte do utworzenia kategorii aplikacji.

7. Określ następujące ustawienia:

   - Algorytm obliczania wartości sumy kontrolnej

W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o obliczonych wartościach sum kontrolnych są przechowywane w bazie danych Serwera administracyjnego. Przechowywanie wartości sum kontrolnych nie zwiększa znacząco rozmiaru bazy danych.

SHA-256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono usterek, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA-256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA-256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA-256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

- Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego, dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA-256 dla plików kategorii.

Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA-256**, jak i pole wyboru **Suma kontrolna MD5**.

Pole **Oblicz sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze)** jest zaznaczone domyślnie.

Pole **Przelicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

- Synchronizuj dane z repozytorium Serwera administracyjnego

Wybierz tę opcję, jeśli chcesz, żeby Serwer administracyjny okresowo sprawdzał zmiany w określonym folderze (lub folderach).

Domyślnie opcja ta jest wyłączona.

Jeśli włączysz tę opcję, określ przedział czasu (w godzinach), aby sprawdzić zmiany w określonym folderze (folderach). Domyślnie przedział czasu skanowania wynosi 24 godziny.

8. W oknie kreatora **Filtr** ogólne określ następujące ustawienia:

- Typ pliku

W tej sekcji możesz określić typ pliku, który jest używany do tworzenia kategorii aplikacji.

Wszystkie pliki. Wszystkie pliki są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

Tylko pliki spoza kategorii aplikacji. Tylko pliki poza kategoriami aplikacji są brane pod uwagę podczas tworzenia kategorii.

- Foldery

W tej sekcji możesz określić, które foldery z wybranego urządzenia (urządzeń) zawierają pliki używane do tworzenia kategorii aplikacji.

Wszystkie foldery. Wszystkie foldery są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

Określony folder. Tylko określony folder jest brany pod uwagę podczas tworzenia kategorii. Jeśli wybierzesz tę opcję, musisz określić ścieżkę do folderu.

9. Na stronie kreatora **Tworzenie kategorii aplikacji** kliknij przycisk **Zakończ**.

Po zakończeniu pracy kreatora tworzona jest kategoria aplikacji użytkownika. Nowo utworzoną kategorię można przejrzeć, korzystając z list kategorii w obszarze roboczym folderu **Kategorie aplikacji**.

Tworzenie kategorii aplikacji zawierającej pliki wykonywalne z określonego folderu

Możesz użyć plików wykonywalnych z wybranego folderu jako standardu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić w swojej organizacji. W oparciu o pliki wykonywalne z wybranego folderu, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji, która zawiera pliki wykonywalne z określonego folderu:

1. W drzewie konsoli, w folderze **Zaawansowane** → **Zarządzanie aplikacjami** wybierz podfolder **Kategorie aplikacji**.

2. Kliknij przycisk **Nowa kategoria**.

   Zostanie uruchomiony **Kreator tworzenia nowej kategorii**. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. Na stronie kreatora **Typ kategorii** wybierz **kategorię, która zawiera pliki wykonywalne z określonego folderu** jako typ kategorii użytkownika.

4. Na stronie kreatora **Wprowadź nazwę kategorii aplikacji** wprowadź nową nazwę kategorii aplikacji.

5. Na stronie kreatora **Folder repozytorium** kliknij przycisk **Przeglądaj**.

6. Określ folder, którego pliki wykonywalne zostaną użyte do utworzenia kategorii aplikacji.

7. Określ następujące ustawienia:

   - Uwzględnij w tej kategorii biblioteki dołączane dynamicznie (DLL)

     Kategoria aplikacji zawiera biblioteki dołączane dynamicznie (pliki w formacie DLL), a moduł Kontrola aplikacji rejestruje akcje takich bibliotek działających w systemie. Włączenie plików DLL do kategorii może obniżyć wydajność Kaspersky Security Center.

     Domyślnie pole to nie jest zaznaczone.

   - Uwzględnij w tej kategorii dane skryptów

Kategoria aplikacji zawiera dane o skryptach, a skrypty nie są blokowane przez moduł Ochrona WWW. Włączenie danych skryptów do kategorii może obniżyć wydajność Kaspersky Security Center.

Domyślnie pole to nie jest zaznaczone.

- Algorytm obliczania wartości sumy kontrolnej: **Oblicz sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze) / Oblicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane przez starsze wersje niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

  W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o obliczonych wartościach sum kontrolnych są przechowywane w bazie danych Serwera administracyjnego. Przechowywanie wartości sum kontrolnych nie zwiększa znacząco rozmiaru bazy danych.

  SHA-256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono usterek, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA-256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

  Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

  - Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA-256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA-256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

  - Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego, dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA-256 dla plików kategorii.

  Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA-256**, jak i pole wyboru **Suma kontrolna MD5**.

  Pole **Oblicz sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze)** jest zaznaczone domyślnie.

  Pole **Przelicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

- Wymuś skanowanie folderu pod kątem zmian

  Jeśli ta opcja jest włączona, aplikacja regularnie sprawdza folder dodawania zawartości kategorii na obecność zmian. Możesz określić częstotliwość skanowań (w godzinach) w polu wejściowym znajdującym się obok pola do zaznaczenia. Domyślnie przedział czasu między wymuszonymi skanowaniami wynosi 24 godziny.

  Jeśli ta opcja jest wyłączona, aplikacja nie wymusza skanowania folderu. Serwer podejmie próbę uzyskania dostępu do plików, jeśli zostały zmodyfikowane, dodane lub usunięte.

  Domyślnie opcja ta jest wyłączona.

8. Na stronie kreatora **Tworzenie kategorii aplikacji** kliknij przycisk **Zakończ**.

Po zakończeniu pracy kreatora tworzona jest kategoria aplikacji użytkownika. Nowo utworzoną kategorię można przejrzeć, korzystając z list kategorii w obszarze roboczym folderu **Kategorie aplikacji**.

Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

Pliki wykonywalne związane ze zdarzeniami **Uruchamianie aplikacji jest zabronione** i **Uruchamianie aplikacji jest zabronione w trybie testowym** możesz dodać do istniejących kategorii aplikacji z zawartością dodaną ręcznie lub do nowej kategorii aplikacji.

W celu dodania plików wykonywalnych związanych ze zdarzeniami Kontroli aplikacji do kategorii aplikacji:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Na zakładce **Zdarzenia** wybierz żądane zdarzenia.
4. Z menu kontekstowego jednego z wybranych zdarzeń wybierz **Dodaj do kategorii**.
5. W otwartym oknie **Akcja na pliku wykonywalnym związanym ze zdarzeniem** określ odpowiednie ustawienia:

   Wybierz jeden z następujących elementów:

   - **Dodaj do nowej kategorii aplikacji**

     Wybierz tę opcję, jeśli chcesz utworzyć nową kategorię aplikacji.

     Kliknij przycisk **OK**, aby uruchomić kreatora nowej kategorii. Po zakończeniu działania kreatora, zostaje utworzona kategoria z określonymi ustawieniami.

     Domyślnie ta opcja nie jest zaznaczona.

   - **Dodaj do istniejącej kategorii aplikacji**

     Wybierz tę opcję, jeśli musisz dodać reguły do istniejącej kategorii aplikacji. Wybierz odpowiednią kategorię na liście kategorii aplikacji.

     Opcja ta jest wybrana domyślnie.

   W sekcji **Rodzaj reguły** wybierz jedno z następujących ustawień:

   - **Dodaj do kategorii**

     Wybierz tę opcję, jeśli musisz dodać reguły do warunków kategorii aplikacji.

     Opcja ta jest wybrana domyślnie.

   - **Reguły dodawania do wykluczeń**

     Wybierz tę opcję, jeśli chcesz dodać reguły do wykluczeń kategorii aplikacji.

   W sekcji **Rodzaj informacji o pliku** wybierz jedno z następujących ustawień:

   - **Szczegóły certyfikatu (lub sumy kontrolne SHA-256 dla plików bez certyfikatu)**

Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

Każdy plik posiada swoją unikatową funkcję skrótu SHA-256. Jeśli wybierzesz funkcję skrótu SHA-256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

Wybierz tę opcję, jeśli chcesz dodać do reguł kategorii szczegóły certyfikatu pliku wykonywalnego (lub funkcję skrótu SHA-256 dla plików bez certyfikatu).

Domyślnie opcja ta jest zaznaczona.

- **Szczegóły certyfikatu (pliki bez certyfikatu zostaną pominięte)**

  Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

  Wybierz tę opcję, jeśli chcesz dodać szczegóły certyfikatu pliku wykonywalnego do reguł kategorii. Jeśli plik wykonywalny nie posiada certyfikatu, ten plik zostanie pominięty. Do kategorii nie zostaną dodane żadne informacje o tym pliku.

- **Tylko SHA-256 (pliki bez sumy kontrolnej zostaną pominięte)**

  Każdy plik posiada swoją unikatową funkcję skrótu SHA-256. Jeśli wybierzesz funkcję skrótu SHA-256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

  Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu SHA-256 pliku wykonywalnego.

- **Tylko MD5 (tryb wycofany, wyłącznie dla wersji Kaspersky Endpoint Security 10 Service Pack 1)**

  Każdy plik posiada swoją unikatową funkcję skrótu MD5. Jeśli wybierzesz funkcję skrótu MD5, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

  Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu MD5 pliku wykonywalnego. Obliczanie funkcji skrótu MD5 jest obsługiwane w Kaspersky Endpoint Security 10 Service Pack 1 for Windows i późniejszych wersjach.

6. Kliknij **OK**.

Konfigurowanie zarządzania uruchamianiem aplikacji na urządzeniach klienckich

Kategoryzacja aplikacji pozwala na optymalizację zarządzania aplikacjami uruchomionymi na urządzeniach. Możesz utworzyć kategorię aplikacji i skonfigurować Kontrolę aplikacji dla profilu, aby uruchomić tylko aplikacje z określonej kategorii na urządzeniach, na których ten profil jest stosowany. Na przykład, możesz utworzyć kategorię, która zawiera aplikacje nazwane *Aplikacja_1* oraz *Aplikacja_2*. Po dodaniu tej kategorii do profilu można uruchamiać tylko dwie aplikacje na urządzeniach, na których stosowany jest profil: *Aplikacja_1* oraz *Aplikacja_2*. Jeśli użytkownik próbuje uruchomić aplikację, która nie została włączona do tej kategorii, na przykład *Aplikacja_3*, uruchomienie tej aplikacji zostaje zablokowane. Użytkownikowi jest wyświetlane powiadomienie informujące, że uruchamianie *Aplikacji_3* jest blokowane, zgodnie z regułą Kontroli aplikacji. Możesz tworzyć kategorie z zawartością dodaną automatycznie na podstawie różnych kryteriów z określonego folderu. W takim przypadku pliki są automatycznie dodawane do kategorii z określonego folderu. Pliki wykonywalne aplikacji są kopiowane do określonego folderu i przetwarzane automatycznie; ich metryki są dodawane do kategorii.

W celu skonfigurowania zarządzania uruchamianiem aplikacji na urządzeniach klienckich:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Kategorie aplikacji**.
2. W obszarze roboczym folderu **Kategorie aplikacji** utwórz kategorię aplikacji, którymi chcesz zarządzać podczas ich uruchamiania.
3. W folderze **Zarządzane urządzenia**, na zakładce **Zasady** kliknij przycisk **Nowa zasada**, aby utworzyć nową zasadę dla Kaspersky Endpoint Security for Windows, i postępuj zgodnie z instrukcjami kreatora.

   Jeśli taki profil już istnieje, możesz pominąć ten krok. W ustawieniach tego profilu możesz skonfigurować zarządzanie uruchamianiem aplikacji w określonej kategorii. Nowo utworzony profil jest wyświetlany w folderze **Zarządzane urządzenia**, na zakładce **Zasady**.
4. Z menu kontekstowego profilu dla Kaspersky Endpoint Security for Windows wybierz **Właściwości**.

   Zostanie otwarte okno właściwości zasady dla Kaspersky Endpoint Security for Windows.
5. W oknie właściwości zasady Kaspersky Endpoint Security for Windows, w sekcji **Kontrola zabezpieczeń** → **Kontrola aplikacji** zaznacz pole **Kontrola aplikacji**.
6. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Reguła Kontroli aplikacji**.
7. W oknie **Reguła Kontroli aplikacji**, z listy rozwijalnej **Kategoria** wybierz kategorię aplikacji, dla których stosowana będzie reguła uruchamiania. Skonfiguruj regułę uruchamiania dla określonej kategorii aplikacji.

   W przypadku Kaspersky Endpoint Security 10 Service Pack 2 i nowszych wersji, żadne kategorie nie są wyświetlane, jeśli zostały utworzone zgodnie z kryterium sumy kontrolnej MD5 pliku wykonywalnego.

   Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA-256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2. Może to spowodować błędy aplikacji.

   Szczegółowe instrukcje dotyczące konfiguracji reguł kontroli można znaleźć w internetowym systemie pomocy dla Kaspersky Endpoint Security for Windows.
8. Kliknij **OK**.

Aplikacje będą uruchamiane na urządzeniach znajdujących się w określonej kategorii zgodnie z regułą, którą utworzyłeś. Nowo utworzona reguła jest wyświetlana w oknie właściwości zasady Kaspersky Endpoint Security for Windows, w sekcji **Kontrola aplikacji**.

Wyświetlanie wyników analizy statycznej reguł uruchamiania zastosowanych na plikach wykonywalnych

W celu wyświetlenia informacji o plikach wykonywalnych, których użytkownicy nie mogą uruchamiać:

1. W folderze **Zarządzane urządzenia** drzewa konsoli wybierz zakładkę **Zasady**.
2. Z menu kontekstowego profilu dla Kaspersky Endpoint Security for Windows wybierz **Właściwości**.

   Zostanie otwarte okno właściwości profilu aplikacji.
3. Na panelu **Sekcje** wybierz **Kontrola zabezpieczeń**, a następnie wybierz podsekcję **Kontrola aplikacji**.
4. Kliknij przycisk **Analiza statyczna**.

   Zostanie otwarte okno **Analiza listy uprawnień dostępu**. W lewej części okna wyświetlana jest lista użytkowników oparta o dane Active Directory.
5. Wybierz użytkownika z listy.

   Prawa część okna wyświetla kategorie aplikacji przypisane do tego użytkownika.
6. Aby wyświetlić pliki wykonywalne, których użytkownik nie może uruchamiać, w oknie **Analiza listy uprawnień dostępu** kliknij przycisk **Wyświetl pliki**.

   Zostanie otwarte okno wyświetlające listę zabronionych plików wykonywalnych.
7. Aby wyświetlić listę plików wykonywalnych z kategorii, wybierz kategorię aplikacji i kliknij przycisk **Wyświetl pliki w kategorii**.

   Zostanie otwarte okno wyświetlające listę plików wykonywanych uwzględnionych w kategorii aplikacji.

Przeglądanie rejestru aplikacji

Kaspersky Security Center przeprowadza inwentaryzację wszystkich programów zainstalowanych na zarządzanych urządzeniach.

Agent sieciowy tworzy listę aplikacji zainstalowanych na urządzeniu, a następnie wysyła ją do Serwera administracyjnego. Agent sieciowy automatycznie pobiera informacje o zainstalowanych aplikacjach z rejestru systemu Windows.

Zbieranie informacji o zainstalowanych aplikacjach jest dostępne tylko dla urządzeń działających pod kontrolą systemu Microsoft Windows.

W celu przeglądania rejestru aplikacji zainstalowanych na urządzeniach klienckich:

W folderze **Zaawansowane → Zarządzanie aplikacjami** w drzewie konsoli wybierz podfolder **Rejestr aplikacji**.

Obszar roboczy folderu **Rejestr aplikacji** wyświetla listę aplikacji zainstalowanych na urządzeniach klienckich i Serwerze administracyjnym.

Możesz wyświetlić szczegóły dowolnej aplikacji, otwierając jej menu kontekstowe i wybierając **Właściwości**. Okno właściwości aplikacji wyświetla szczegóły dotyczące aplikacji oraz informacje o jej plikach wykonywalnych, a także listę urządzeń, na których zainstalowano aplikację.

W menu kontekstowym dowolnej aplikacji na liście możesz:

- Dodać tę aplikację do kategorii aplikacji.

- Przypisać znacznik do aplikacji.
- Wyeksportować listę aplikacji do pliku CSV lub pliku TXT.
- Przeglądać właściwości aplikacji, na przykład, nazwę producenta, numer wersji, listę plików wykonywalnych, listę urządzeń, na których jest zainstalowana aplikacja, listę dostępnych aktualizacji oprogramowania lub listę wykrytych luk w oprogramowaniu.

Aby wyświetlić aplikacje spełniające określone kryteria, można użyć filtrowania w obszarze roboczym folderu **Rejestr aplikacji**.

W oknie właściwości wykrytego urządzenia, w sekcji **Rejestr aplikacji** możesz przejrzeć listę aplikacji zainstalowanych na urządzeniu.

Generowanie raportu dotyczącego zainstalowanych aplikacji

W obszarze roboczym **Rejestr aplikacji** możesz także kliknąć przycisk **Wyświetl raport o zainstalowanych aplikacjach**, aby wygenerować raport zawierający szczegółowe statystyki dotyczące zainstalowanych aplikacji, w tym liczbę urządzeń, na których każda aplikacja jest zainstalowana. Ten raport, który otwiera stronę **Raport o zainstalowanych aplikacjach**, zawiera informacje o aplikacjach firmy Kaspersky oraz o oprogramowaniu innych firm. Jeśli chcesz tylko informacji na temat aplikacji firmy Kaspersky, zainstalowanych na urządzeniach klienckich, z listy **Podsumowanie** wybierz AO Kaspersky Lab.

Również informacje o aplikacjach Kaspersky i oprogramowaniu firm trzecich zainstalowanych na urządzeniach podłączonych do podrzędnych i wirtualnych Serwerów administracyjnych są przechowywane w rejestrze aplikacji głównego Serwera administracyjnego. Po dodaniu danych z podrzędnych i wirtualnych Serwerów administracyjnych, kliknij przycisk **Wyświetl raport o zainstalowanych aplikacjach**, a na stronie **Raport o zainstalowanych aplikacjach**, która zostanie otwarta, będziesz mógł przejrzeć te informacje.

W celu dodania informacji z podrzędnych i wirtualnych Serwerów administracyjnych do raportu o zainstalowanych aplikacjach:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na zakładce **Raporty** wybierz **Raport o zainstalowanych aplikacjach**.
4. Z menu kontekstowego raportu wybierz **Właściwości**.

   Zostanie otwarte okno **Właściwości: Raport o zainstalowanych aplikacjach**.
5. W sekcji **Hierarchia Serwerów administracyjnych** zaznacz pole **Dołącz dane z podrzędnych i wirtualnych Serwerów administracyjnych**.
6. Kliknij **OK**.

   Informacje z podrzędnych i wirtualnych Serwerów administracyjnych będą uwzględnione w **Raport o zainstalowanych aplikacjach**.

Zmienianie czasu uruchomienia inwentaryzacji oprogramowania

Kaspersky Security Center przeprowadza inwentaryzację wszystkich programów zainstalowanych na zarządzanych urządzeniach klienckich działających pod kontrolą systemu Windows.

Agent sieciowy tworzy listę aplikacji zainstalowanych na urządzeniu, a następnie wysyła ją do Serwera administracyjnego. Agent sieciowy automatycznie pobiera informacje o zainstalowanych aplikacjach z rejestru systemu Windows.

Aby zapisać zasoby urządzenia, domyślnie Agent sieciowy rozpoczyna pobieranie informacji o zainstalowanych aplikacjach 10 minut po uruchomieniu usługi Agenta sieciowego.

W celu zmiany czasu uruchomienia inwentaryzacji oprogramowania, który upłynie po uruchomieniu usługi Agenta sieciowego na urządzeniu:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Agent sieciowy (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).
2. Przejdź do gałęzi:
   - W systemach 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - W systemach 64-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. Dla klucza KLINV_INV_COLLECTOR_START_DELAY_SEC ustaw żądaną wartość w sekundach.

   Domyślna wartość to 600 sekund.
4. Uruchom ponownie usługę Agenta sieciowego.

Czas uruchomienia inwentaryzacji oprogramowania, który upłynie po uruchomieniu usługi Agenta sieciowego, zostanie zmieniony.

Informacje o zarządzaniu kluczem licencyjnym dla aplikacji innych firm

Kaspersky Security Center umożliwia śledzenie użycia klucza licencyjnego przez aplikacje firm trzecich zainstalowane na zarządzanych urządzeniach. Lista aplikacji, dla których można śledzić użycie klucza licencyjnego, jest pobierana z rejestru aplikacji. Dla każdego klucza licencyjnego można określić i śledzić naruszenie następujących ograniczeń:

- Maksymalna liczba urządzeń, na których aplikacja korzystająca z tego klucza licencyjnego może zostać zainstalowana
- Data wygaśnięcia klucza licencyjnego

Kaspersky Security Center nie sprawdza, czy określiłeś prawdziwy klucz licencyjny. Możesz śledzić tylko określone przez siebie ograniczenia. Jeśli jedno z ograniczeń, które nakładasz na klucz licencyjny, zostanie naruszone, Serwer administracyjny zarejestruje zdarzenie informacyjne, ostrzeżenie lub błąd funkcjonalny.

Klucze licencyjne są powiązane z grupami aplikacji. Grupa aplikacji to grupa aplikacji innych firm, które łączysz na podstawie jednego lub kilku kryteriów. Aplikacje można definiować według nazwy aplikacji, jej wersji, producenta i znacznika. Aplikacja jest dodawana do grupy, jeśli przynajmniej jedno z kryteriów jest spełnione. Do każdej grupy aplikacji można przypisać kilka kluczy licencyjnych, ale każdy klucz licencyjny może być powiązany tylko z jedną grupą aplikacji.

Kolejnym narzędziem, którego można użyć do śledzenia użycia klucza licencyjnego, jest Raport o stanie dotyczącym grup licencjonowanych aplikacji. Ten raport zawiera informacje o aktualnym stanie grup licencjonowanych aplikacji, w tym:

- Liczba instalacji kluczy licencyjnych w każdej grupie aplikacji
- Liczba używanych kluczy licencyjnych i wolnych kluczy licencyjnych
- Szczegółowa lista licencjonowanych aplikacji zainstalowanych na zarządzanych urządzeniach

Narzędzia do zarządzania kluczami licencyjnymi aplikacji innych firm znajdują się w podfolderze **Wykorzystanie licencji firm trzecich** (**Zaawansowane →Zarządzanie aplikacjami →Wykorzystanie licencji firm trzecich**). W tym podfolderze można tworzyć grupy aplikacji, dodawać klucze licencyjne i generować Raport o statnach grup licencjonowanych aplikacji.

Narzędzia do zarządzania kluczami licencyjnymi aplikacji innych firm są dostępne tylko po włączeniu opcji Zarządzanie lukami i poprawkami w oknie **Konfiguruj interfejs**.

Tworzenie grup licencjonowanych aplikacji

W celu utworzenia grupy licencjonowanych aplikacji:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Wykorzystanie licencji firm trzecich**.
2. Kliknij przycisk **Dodaj grupę licencjonowanych aplikacji**, aby uruchomić Kreator dodawania grupy licencjonowanych aplikacji.

   Zostanie uruchomiony Kreator dodawania grupy licencjonowanych aplikacji.
3. W kroku **Szczegóły grupy licencjonowanych aplikacji** określ, które aplikacje chcesz uwzględnić w grupie aplikacji:
   - **Nazwa grupy licencjonowanych aplikacji**
   - Śledź naruszenia ograniczeń

Jeśli jedno z ograniczeń, które nakładasz na klucz licencyjny grupy aplikacji, zostanie naruszone, Serwer administracyjny zarejestruje zdarzenie informacyjne, ostrzeżenie lub błąd funkcjonalny:

- Zdarzenie informacyjne: **Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony (wykorzystywanych jest więcej niż 95%)**
- Ostrzeżenie: **Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony**
- Błąd funkcjonalny: **Przekroczono limit instalacji dla jednej z grup licencjonowanych aplikacji**

  Zdarzenie jest rejestrowane tylko raz, gdy określony warunek zostanie spełniony. Następnym razem to samo zdarzenie można zarejestrować tylko wtedy, gdy liczba instalacji powróci do normalnego poziomu, po czym zdarzenie wystąpi ponownie. Nie można zarejestrować zdarzenia częściej niż raz na godzinę.

- Kryteria dodawania wykrytych aplikacji do tej grupy licencjonowanych aplikacji

  Określ kryteria, aby zdefiniować aplikacje, które chcesz uwzględnić w grupie aplikacji. Aplikacje można definiować według nazwy aplikacji, jej wersji, producenta i znacznika. Musisz określić co najmniej jedno kryterium. Aplikacja jest dodawana do grupy, jeśli przynajmniej jedno z kryteriów jest spełnione.

4. W kroku **Wprowadź dane o istniejących kluczach licencyjnych** określ klucze licencyjne, które chcesz śledzić. Wybierz opcję **Kontroluj, jeśli limit licencji zostanie przekroczony**, a następnie dodaj klucze licencyjne:

   a. Kliknij przycisk **Dodaj**.

   b. Wybierz klucz licencyjny, który chcesz dodać, a następnie kliknij przycisk **OK**. Jeśli wymaganego klucza licencyjnego nie ma na liście, kliknij przycisk **Dodaj**, a następnie określ właściwości klucza licencyjnego.

5. W kroku **Dodaj grupę licencjonowanych aplikacji** kliknij przycisk **Zakończ**.

Grupa licencjonowanych aplikacji zostanie utworzona i wyświetlona w folderze **Wykorzystanie licencji firm trzecich**.

Zarządzanie kluczami licencyjnymi dla grup licencjonowanych aplikacji

W celu utworzenia klucza licencyjnego dla grupy licencjonowanych aplikacji:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Wykorzystanie licencji firm trzecich**.

2. W obszarze roboczym folderu **Wykorzystanie licencji firm trzecich** kliknij przycisk **Zarządzaj kluczami licencjonowanych aplikacji**.

   Zostanie otwarte okno **Zarządzanie kluczami licencjonowanych aplikacji**.

3. W oknie **Zarządzanie kluczami licencjonowanych aplikacji** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Klucz licencyjny**.

4. W oknie **Klucz licencyjny** określ właściwości klucza licencyjnego i ograniczenia, jakie ten klucz licencyjny nakłada na grupę licencjonowanych aplikacji.

- **Nazwa**. Nazwa klucza licencyjnego.
- **Komentarz**. Komentarz dotyczący wybranego klucza licencyjnego.
- **Ograniczenie**. Liczba urządzeń, na których aplikacja korzystająca z tego klucza licencyjnego może zostać zainstalowana.
- **Utraci ważność**. Data wygaśnięcia klucza licencyjnego.

Utworzone klucze są wyświetlane w oknie **Zarządzanie kluczami licencjonowanych aplikacji**.

W celu zastosowania klucza licencyjnego do grupy licencjonowanych aplikacji:

1. W folderze **Zaawansowane → Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Wykorzystanie licencji firm trzecich**.
2. W folderze **Wykorzystanie licencji firm trzecich** wybierz grupę licencjonowanych aplikacji, dla której chcesz zastosować klucz licencyjny.
3. Z menu kontekstowego grupy licencjonowanych aplikacji wybierz polecenie **Właściwości**.

   Zostanie otwarte okno właściwości grupy licencjonowanych aplikacji.
4. W oknie właściwości grupy licencjonowanych aplikacji, w sekcji **Klucze licencyjne** wybierz **Kontroluj, jeśli limit licencji zostanie przekroczony**.
5. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Wybierz klucz licencyjny**.
6. W oknie **Wybierz klucz licencyjny** wybierz klucz licencyjny, który chcesz zastosować do grupy licencjonowanych aplikacji.
7. Kliknij **OK**.

Ograniczenia nałożone na grupę licencjonowanych aplikacji i określone w kluczu licencyjnym będą zastosowane do wybranej grupy licencjonowanych aplikacji.

Inwentaryzacja plików wykonywalnych

Możesz użyć zadania inwentaryzacji do przeprowadzenia inwentaryzacji plików wykonywalnych na urządzeniach klienckich. Kaspersky Endpoint Security for Windows oferuje funkcję inwentaryzacji plików wykonywalnych.

Liczba plików wykonywalnych pobranych z jednego urządzenia nie może przekraczać 150 000. Po osiągnięciu tego limitu, Kaspersky Security Center nie będzie mógł otrzymywać nowych plików.

Zanim zaczniesz, włącz powiadomienia o uruchamianiu aplikacji w profilu Kaspersky Endpoint Security oraz w profilu Agenta sieciowego, aby móc przesłać dane do Serwera administracyjnego.

Aby włączyć powiadomienia o uruchomieniu aplikacji:

- Otwórz ustawienia zasad Kaspersky Endpoint Security i wykonaj następujące czynności:

1. Przejdź do **Ustawienia ogólne → Raporty i przechowywanie**.
2. W sekcji **Transfer danych do Serwera administracyjnego** zaznacz pole **Informacje o uruchomionych aplikacjach**.
3. Zapisz zmiany.

- Otwórz ustawienia zasad Agenta sieciowego i wykonaj następujące czynności:
  1. Przejdź do sekcji **Repozytoria**.
  2. Zaznacz pole wyboru **Szczegóły zainstalowanych aplikacji**.
  3. Zapisz zmiany.

W celu utworzenia zadania dla plików wykonywalnych na urządzeniach klienckich:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Kliknij przycisk **Nowe zadanie** w obszarze roboczym folderu **Zadania**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W oknie **Wybierz typ zadania**, jako typ zadania wybierz **Kaspersky Endpoint Security**, a następnie, jako podtyp zadania wskaż **Inwentaryzacja** i kliknij **Dalej**.
4. Wykonaj pozostałe instrukcje kreatora.

   Po zakończeniu pracy kreatora zostanie utworzone zadanie inwentaryzacji dla Kaspersky Endpoint Security. Nowo utworzone zadanie będzie wyświetlane na liście zadań, w obszarze roboczym folderu **Zadania**.

Lista plików wykonywalnych, wykrytych na urządzeniach podczas inwentaryzacji, jest wyświetlana w obszarze roboczym folderu **Pliki wykonywalne**.

Podczas inwentaryzacji aplikacja wykrywa pliki wykonywalne w następujących formatach: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR oraz HTML.

Przeglądanie informacji o plikach wykonywalnych

W celu przejrzenia listy wszystkich plików wykonywalnych wykrytych na urządzeniach klienckich:

W folderze **Zarządzanie aplikacjami** drzewa konsoli wybierz podfolder **Pliki wykonywalne**.

Obszar roboczy folderu **Pliki wykonywalne** wyświetla listę plików wykonywalnych uruchomionych na urządzeniach od momentu zainstalowania systemu operacyjnego, bądź też plików wykrytych podczas działania zadania inwentaryzacji programu Kaspersky Endpoint Security for Windows.

Aby wyświetlić szczegóły dotyczące plików wykonywalnych spełniających określone kryteria, możesz użyć filtrowania.

W celu przejrzenia właściwości pliku wykonywalnego:

Wybierając z menu kontekstowego pliku element **Właściwości**.

Zostanie otwarte okno wyświetlające informacje o pliku wykonywalnym oraz listę urządzeń, na których wykryto plik wykonywalny.

Monitorowanie i raportowanie

Ta sekcja opisuje możliwości monitorowania i raportowania Kaspersky Security Center. Te możliwości dają ogląd infrastruktury, stanów ochrony i statystyk.

Po zainstalowaniu programu Kaspersky Security Center lub podczas jego działania, możesz skonfigurować funkcje monitorowania i raportowania, aby najlepiej odpowiadały Twoim potrzebom.

- **Kolory wskaźnika**

  Konsola administracyjna umożliwia szybką ocenę bieżącego stanu Kaspersky Security Center i zarządzanych urządzeń poprzez sprawdzenie wskaźników przypominających sygnalizację świetlną.

- **Statystyki**

  Statystyki dotyczące stanu systemu ochrony i zarządzanych urządzeń są wyświetlane w panelach informacyjnych, które można dostosować.

- **Raporty**

  Raporty umożliwiają uzyskanie szczegółowych informacji liczbowych na temat ochrony sieci Twojej organizacji, zapisania tych informacji w pliku, wysłania ich w wiadomości e-mail oraz ich wydrukowania.

- **Zdarzenia**

  Wybory zdarzeń oferują widok ekranowy nazwanych zestawów zdarzeń, które są wybrane z bazy danych Serwera administracyjnego. Te zestawy zdarzeń są grupowane zgodnie z następującymi kategoriami:

  - Według istotności—**Zdarzenia krytyczne**, **Błędy funkcjonalne**, **Ostrzeżenia** i **Informacja o zdarzeniach**
  - Według czasu—**Ostatnie zdarzenia**
  - Według typu—**Żądania użytkownika** and **Zdarzenia audytu**

Możesz tworzyć i przeglądać wybory zdarzeń zdefiniowane przez użytkownika oparte na ustawieniach dostępnych do konfiguracji w interfejsie Kaspersky Security Center Web Console.

Scenariusz: Monitorowanie i raportowanie

Ta sekcja zawiera scenariusz konfigurowania funkcji monitorowania i raportowania w Kaspersky Security Center.

Wymagania wstępne

Po wdrożeniu Kaspersky Security Center w sieci organizacji, możesz uruchomić jej monitorowanie i wygenerować raporty dotyczące jej funkcjonowania.

Etapy

Monitorowanie i raportowanie w sieci organizacji odbywa się w etapach:

1. **Konfigurowanie przełączania stanów urządzeń**

   Zapoznaj się z ustawieniami, które definiują przypisywanie stanów urządzeń w zależności od określonych warunków. Zmieniając te ustawienia, możesz zmienić liczbę zdarzeń z priorytetami *Krytyczne* lub *Ostrzeżenie*.

   Podczas konfigurowania przełączania stanów urządzeń upewnij się, że nowe ustawienia nie kolidują z zasadami bezpieczeństwa informacji Twojej organizacji i że nie możesz reagować na ważne zdarzenia związane z bezpieczeństwem w sieci w Twojej organizacji w odpowiednim momencie.

2. **Konfigurowanie powiadomień o zdarzeniach występujących na urządzeniach klienckich**

   Skonfiguruj powiadamianie (poprzez e-mail, wiadomość SMS lub przez uruchomienie pliku wykonywalnego) o zdarzeniach na urządzeniach klienckich zgodnie z potrzebami Twojej organizacji.

3. **Zmiana reakcji ochrony sieci na zdarzenie Epidemia wirusa**

   Aby dostosować odpowiedź sieci na nowe zdarzenia, możesz zmienić określone wartości progowe we właściwościach Serwera administracyjnego. Możesz także utworzyć rygorystyczną zasadę, która zostanie aktywowana, lub utworzyć zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.

4. **Zarządzanie statystykami**

   Skonfiguruj wyświetlanie statystyk zgodnie z potrzebami Twojej organizacji.

5. **Sprawdzanie stanu ochrony sieci w swojej organizacji**

   W celu przejrzenia stanu ochrony sieci w Twojej organizacji możesz wykonać jedną z następujących czynności:

   - W obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Statystyki** otwórz zakładkę drugiego poziomu (stronę) **Stan ochrony** i przejrzyj panel informacyjny **Stan ochrony w czasie rzeczywistym**
   - Wygeneruj i sprawdź **Raport o stanie ochrony**
   - Wygeneruj i przejrzyj **Raport o błędach**

6. **Lokalizowanie urządzeń klienckich, które nie są chronione**

   Aby zlokalizować urządzenia klienckie, które nie są chronione, przejdź do obszaru roboczego węzła **Serwer administracyjny**, na zakładce **Statystyki** otwórz zakładkę drugiego poziomu (stronę) **Stan ochrony** i przejrzyj panel informacyjny **Historia wykrywania nowych urządzeń w sieci**. Możesz także wygenerować i przejrzeć **Raport wdrażania ochrony**.

7. **Sprawdzanie ochrony urządzeń klienckich**

   Aby sprawdzić ochronę urządzeń klienckich, przejdź do obszaru roboczego węzła **Serwer administracyjny**, na zakładce **Statystyki** otwórz zakładkę drugiego poziomu (stronę) **Wdrażanie** lub **Statystyki zagrożeń** i przejrzyj odpowiednie panele informacyjne. Możesz także uruchomić i przejrzeć wybór zdarzeń **Zdarzenia krytyczne**.

8. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Aby ocenić obciążenie bazy danych zdarzeniami, oblicz miejsce w bazie danych. Możesz także ograniczyć maksymalną liczbę zdarzeń, aby uniknąć przepełnienia bazy danych.

9. **Przeglądanie informacji o licencji**

   Aby przejrzeć informacje o licencji, przejdź do obszaru roboczego węzła **Serwer administracyjny**, na zakładce **Statystyki** otwórz zakładkę drugiego poziomu (stronę) **Wdrażanie** i przejrzyj panel informacyjny **Użycie kluczy licencyjnych**. Możesz także wygenerować i przejrzeć **Raport o użyciu kluczy licencyjnych**.

Wyniki

Po zakończeniu scenariusza zostaniesz poinformowany o ochronie sieci w swojej organizacji i tym samym będziesz mógł zaplanować działania związane z dalszą ochroną.

Kolory ikony wskaźnika w Konsoli administracyjnej

Konsola administracyjna umożliwia szybką ocenę bieżącego stanu Kaspersky Security Center i zarządzanych urządzeń poprzez sprawdzenie wskaźników przypominających sygnalizację świetlną. Kolory wskaźnika są pokazywane w obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Monitorowanie**. Zakładka udostępnia sześć paneli informacyjnych ze wskaźnikami. Wskaźnik to kolorowy, pionowy pasek po lewej stronie panelu. Każdy panel ze wskaźnikiem odpowiada określonym zakresom funkcjonalnym Kaspersky Security Center (patrz tabela poniżej).

Kolory ikony wskaźnika w Konsoli administracyjnej

Nazwa panelu	Zakres funkcji
Wdrażanie	Instalacja Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci organizacji
Schemat zarządzania	Struktura grup administracyjnych. Skanowanie sieci. Reguły przenoszenia urządzeń
Ustawienia ochrony	Funkcjonalność aplikacji zabezpieczającej: stan ochrony, skanowanie w poszukiwaniu złośliwego oprogramowania
Aktualizacja	Uaktualnienia i łaty
Monitorowanie	Stan ochrony
Serwer administracyjny	Funkcje Serwera administracyjnego i właściwości

Każdy wskaźnik może przyjąć jeden z pięciu kolorów (patrz tabela poniżej). Kolor wskaźnika zależy od aktualnego stanu Kaspersky Security Center i zdarzeń, które zostały zarejestrowane.

Kolory zestawów

Stan	Kolor wskaźnika	Znaczenie koloru wskaźnika
Informacja	Zielony	Nie jest wymagana interwencja administratora.
Ostrzeżenie	Żółty	Wymagana jest interwencja administratora.
Krytyczny	Czerwony	Wystąpiły poważne problemy. W celu rozwiązania tych problemów wymagana jest interwencja administratora.
Informacja	Niebieski	Wydarzenia, które zostały zarejestrowane, nie są związane z potencjalnymi lub rzeczywistymi zagrożeniami dla bezpieczeństwa zarządzanych urządzeń.
Informacja	Szary	Szczegóły zdarzeń są niedostępne lub nie zostały jeszcze pobrane.

Celem administratora jest zachowanie zielonych kolorów wskaźników na wszystkich panelach informacyjnych, na zakładce **Monitorowanie**.

Praca z raportami, statystykami i powiadomieniami

Ta sekcja zawiera informacje dotyczące sposobów pracy z raportami, statystykami i wyborami zdarzeń i urządzeń w Kaspersky Security Center, jak również informacje o konfigurowaniu powiadomień Serwera administracyjnego.

Praca z raportami

Raporty w Kaspersky Security Center zawierają informacje o stanie zarządzanych urządzeń. Raporty są generowane na podstawie informacji przechowywanych na Serwerze administracyjnym. Możesz utworzyć raporty dla następujących typów obiektów:

- Dla wyborów urządzeń utworzonych zgodnie z określonymi ustawieniami.
- Dla grup administracyjnych.
- Dla określonych urządzeń należących do różnych grup administracyjnych.
- Dla wszystkich urządzeń w sieci (w raporcie rozsyłania).

Aplikacja oferuje kilka sztandarowych szablonów raportów. Możliwe jest utworzenie swoich własnych szablonów raportów. Raporty są wyświetlane w oknie głównym aplikacji, w folderze **Serwer administracyjny**.

Tworzenie szablonu raportu

W celu utworzenia szablonu raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Kliknij przycisk **Nowy szablon raportu**.

   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu pracy kreatora, nowo utworzony szablon raportu jest dodawany do wybranego folderu **Serwer administracyjny** drzewa konsoli. Możesz użyć tego szablonu do generowania i wyświetlania raportów.

Przeglądanie i edytowanie właściwości szablonu raportu

Możesz przeglądać i edytować podstawowe właściwości szablonu raportu, na przykład, nazwę szablonu raportu lub pola wyświetlane w raporcie.

W celu przejrzenia i edytowania właściwości szablonu raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu wybierz żądany szablon raportu.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Właściwości**.

Alternatywnie możesz w pierwszej kolejności wygenerować raport, a następnie kliknąć przycisk **Otwórz właściwości szablonu raportu** lub przycisk **Konfiguruj kolumny raportu**.

5. W otwartym oknie edytuj właściwości szablonu raportu. Właściwości każdego raportu mogą zawierać tylko pewne sekcje opisane poniżej.

   - **Sekcja Ogólny**:

     - Nazwa szablonu raportu

     - Maksymalna liczba wyświetlanych wpisów

       Jeśli ta opcja jest włączona, liczba wpisów wyświetlanych w tabeli ze szczegółowymi danymi raportu nie wynosi więcej niż określona wartość.

       Wpisy w raporcie są najpierw przechowywane zgodnie z regułami określonymi w sekcji **Pola → Pola szczegółów** właściwości szablonu raportu, a następnie przechowywane są tylko pierwsze wpisy wynikowe. Nagłówek tabeli ze szczegółowymi danymi raportu pokazuje wyświetloną liczbę wpisów oraz całkowitą dostępną liczbę wpisów, które odpowiadają ustawieniom innego szablonu raportu.

       Jeśli ta opcja jest wyłączona, tabela ze szczegółowymi danymi raportu wyświetla wszystkie dostępne wpisy. Nie jest zalecane wyłączenie tej opcji. Ograniczenie liczby wyświetlanych wpisów raportu zmniejsza obciążenie systemu zarządzania bazą danych (DBMS) i skraca czas wymagany do wygenerowania i eksportowania raportu. Niektóre z raportów zawierają zbyt wiele wpisów. W takiej sytuacji może być trudno przeczytać i przeanalizować je wszystkie. Dodatkowo, podczas tworzenia takiego raportu, na Twoim urządzeniu może zabraknąć pamięci, co w konsekwencji uniemożliwi przejrzenie raportu.

       Domyślnie opcja ta jest włączona. Domyślna wartość to 1000.

     - Wersja do druku

       Raport wyjściowy jest zoptymalizowany do drukowania: znaki spacji zostały dodane między niektórymi wartościami dla lepszej widoczności.

       Domyślnie opcja ta jest włączona.

   - Sekcja **Pola**

     Wybierz pola, które będą wyświetlane w raporcie, oraz kolejność tych pól, a także skonfiguruj, czy informacje w raporcie muszą być sortowane i filtrowane według każdego z pól.

   - Sekcja **Przedział czasu**

     Zmodyfikuj okres dla raportu. Dostępne wartości wyglądają następująco:

     - Między dwoma określonymi datami
     - Od określonej daty do daty utworzenia raportu
     - Od daty utworzenia raportu minus określona liczba dni do daty utworzenia raportu

   - Sekcja **Grupa**, **Wybór urządzeń** lub **Urządzenia.**

     Zmień zestaw urządzeń klienckich, dla których tworzony jest raport. Tylko jedna z tych sekcji może być obecna, w zależności od ustawień określonych podczas tworzenia szablonu raportu.

   - Sekcja **Ustawienia**.

     Zmień ustawienia raportu. Dokładny zestaw ustawień zależy od określonego raportu.

- Sekcja **Zabezpieczenia**. Dziedzicz ustawienia od Serwera administracyjnego

  Jeśli ta opcja jest włączona, ustawienia zabezpieczeń raportu są dziedziczone od Serwera administracyjnego.

  Jeśli ta opcja jest wyłączona, możesz skonfigurować ustawienia zabezpieczeń dla raportu. Możesz przypisać rolę do użytkownika lub grupy użytkowników lub przypisać uprawnienia do użytkownika lub grupy użytkowników, jak zastosowano do raportu.

  Domyślnie opcja ta jest włączona.

  Sekcja **Zabezpieczenia** jest dostępna, jeśli w oknie ustawień interfejsu dostępne jest pole **Wyświetl sekcje ustawień zabezpieczeń**.

- Sekcja **Hierarchia Serwerów administracyjnych**

  - Dołącz dane z podrzędnych i wirtualnych Serwerów administracyjnych

    Jeśli ta opcja jest włączona, raport zawiera informacje z podrzędnych i wirtualnych Serwerów administracyjnych, które podlegają Serwerowi administracyjnemu, dla którego utworzono szablon raportu.

    Wyłącz tę opcję, jeśli chcesz przejrzeć dane tylko z bieżącego Serwera administracyjnego.

    Domyślnie opcja ta jest włączona.

  - Do poziomu zagnieżdżenia

    Raport zawiera dane z podrzędnych i wirtualnych Serwerów administracyjnych, które znajdują się pod bieżącym Serwerem administracyjnym na poziomie zagnieżdżenia, który jest mniejszy niż lub równy określonej wartości.

    Domyślna wartość to 1. Możesz chcieć zmienić tę wartość, jeśli musisz zbierać informacje z podrzędnych Serwerów administracyjnych znajdujących się na niższych poziomach drzewa.

  - Czas oczekiwania na dane (min)

    Przed wygenerowaniem raportu, Serwer administracyjny, dla którego tworzony jest szablon raportu, oczekuje na dane z podrzędnych Serwerów administracyjnych przez określoną liczbę minut. Jeśli żadne dane nie są pobierane z podrzędnego Serwera administracyjnego pod koniec tego okresu, raport i tak zostanie uruchomiony. Zamiast rzeczywistych danych, raport wyświetla dane pobrane z pamięci podręcznej (jeśli opcja **Buforuj dane z podrzędnych Serwerów administracyjnych** jest włączona) lub **N/A** (nie jest dostępne) w innym przypadku.

    Domyślna wartość to 5 (minuty).

  - Buforuj dane z podrzędnych Serwerów administracyjnych

Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Przesłane dane są przechowywane w pamięci podręcznej.

Jeśli podczas generowania raportu bieżący Serwer administracyjny nie może odbierać danych z podrzędnego Serwera administracyjnego, raport wyświetla dane pobrane z pamięci podręcznej. Wyświetlana jest także data przesłania danych do pamięci podręcznej.

Włączenie tej opcji umożliwia przeglądanie informacji z podrzędnych Serwerów administracyjnych nawet wtedy, gdy aktualne dane nie mogą zostać pobrane. Jednakże wyświetlane dane mogą być przestarzałe.

Domyślnie opcja ta jest wyłączona.

- **Częstotliwość aktualizacji pamięci podręcznej (godz.)**

  Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Możesz określić ten okres w godzinach. Jeśli określisz 0 godzin, dane są przesyłane tylko wtedy, gdy raport zostaje wygenerowany.

  Domyślna wartość to 0.

- **Prześlij szczegółowe informacje z podrzędnych Serwerów administracyjnych**

  W wygenerowanym raporcie tabela ze szczegółowymi danymi raportu zawiera dane z podrzędnych Serwerów administracyjnych Serwera administracyjnego, dla którego został utworzony szablon raportu.

  Włączenie tej opcji spowalnia tworzenie raportu i zwiększa ruch sieciowy między Serwerami administracyjnymi. Jednakże możesz przejrzeć wszystkie dane w jednym raporcie.

  Zamiast włączyć tę opcję, możesz chcieć przeanalizować szczegółowe dane raportu, aby wykryć wadliwy podrzędny Serwer administracyjny, a następnie wygenerować ten sam raport tylko dla tego wadliwego Serwera administracyjnego.

  Domyślnie opcja ta jest wyłączona.

Rozszerzony format filtra w szablonach raportu

W Kaspersky Security Center 14.2 możesz zastosować rozszerzony format filtra do szablonu raportu. Rozszerzony format filtra zapewnia większą elastyczność w porównaniu z domyślnym formatem. Możesz utworzyć złożone warunki filtrowania przy użyciu zestawu filtrów, które będą stosowane do raportu przy użyciu operatora logicznego LUB podczas tworzenia raportu w sposób opisany poniżej:

Filter[1](Field[1] AND Field[2]... AND Field[n]) OR Filter[2](Field[1] AND Field[2]... AND Field[n]) OR... Filter[n](Field[1] AND Field[2]... AND Field[n])

Dodatkowo, przy użyciu rozszerzonego formatu filtra możesz określić wartość przedziału czasu w odpowiednim formacie czasu (na przykład, korzystając z warunku „Przez ostatnie N dni") dla określonych pól w filtrze. Dostępność i zestaw warunków przedziału czasu zależy od typu szablonu raportu.

Konwertowanie filtra do rozszerzonego formatu

Format rozszerzonego filtra dla szablonów raportów jest obsługiwany tylko w Kaspersky Security Center 12 i nowszych wersjach. Po konwersji domyślnego filtra do rozszerzonego formatu, szablon raportu stanie się niekompatybilny z Serwerami administracyjnymi w Twojej sieci, w której znajdują się zainstalowane wcześniejsze wersje Kaspersky Security Center. Informacje z tych Serwerów administracyjnych nie zostaną odebrane dla raportu.

W celu przekonwertowania domyślnego filtra szablonu raportu do formatu rozszerzonego:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu wybierz żądany szablon raportu.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Właściwości**.
5. W otwartym oknie właściwości wybierz sekcję **Pola**.
6. Na zakładce **Pola szczegółów** kliknij odnośnik **Konwertuj filtr**.
7. W otwartym oknie kliknij przycisk **OK**.

   Konwersja do rozszerzonego formatu filtra jest nieodwracalna dla szablonu raportu, do którego jest stosowana. Jeśli kliknąłeś odnośnik **Konwertuj filtr** przez przypadek, możesz anulować wprowadzone zmiany poprzez kliknięcie przycisku **Anuluj** w oknie właściwości szablonu raportu.

8. Aby zastosować wprowadzone zmiany, zamknij okno właściwości szablonu raportu, klikając przycisk **OK**.

   Jeśli okno właściwości szablonu raportu zostanie otwarte ponownie, zostanie wyświetlona nowo dostępna sekcja **Filtry**. W tej sekcji możesz skonfigurować rozszerzony filtr.

Konfigurowanie rozszerzonego filtra

W celu skonfigurowania rozszerzonego filtra we właściwościach szablonu raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportów wybierz szablon raportu, który wcześniej został przekonwertowany do formatu rozszerzonego filtra.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Właściwości**.
5. W otwartym oknie właściwości wybierz sekcję **Filtry**.

   Sekcja **Filtry** nie jest wyświetlana, jeśli szablon raportu nie został wcześniej przekonwertowany do formatu rozszerzonego filtra.

   W sekcji **Filtry** okna właściwości szablonu raportu możesz przejrzeć i zmodyfikować listę filtrów stosowanych do raportu. Każdy filtr na liście posiada unikatową nazwę i przedstawia zestaw filtrów dla odpowiednich pól w raporcie.

6. Otwórz okno ustawień filtra w jeden z następujących sposobów:

   - Aby utworzyć nowy filtr, kliknij przycisk **Dodaj**.

- Aby zmodyfikować istniejący filtr, wybierz żądany filtr i kliknij przycisk **Modyfikuj**.

7. W otwartym oknie wybierz i określ wartości wymaganych pól filtra.
8. Aby zapisać wprowadzone zmiany i zamknąć okno, kliknij przycisk **OK**.

   Jeśli tworzysz nowy filtr, nazwa filtra musi zostać określona w polu **Nazwa filtra** przed kliknięciem przycisku **OK**.
9. Zamknij okno właściwości szablonu raportu, klikając przycisk **OK**.

   Rozszerzony filtr w szablonie raportu zostanie skonfigurowany. Teraz możesz tworzyć raporty, korzystając z szablonu raportu.

Tworzenie i przeglądanie raportu

W celu utworzenia i przejrzenia raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu kliknij dwukrotnie żądany szablon raportu.

   Zostanie wyświetlony raport dla wybranego szablonu.

Raport wyświetla następujące dane:

- Nazwę i typ raportu, krótki opis i okres raportowania, a także informacje o grupie urządzeń, dla których generowany jest raport.
- Wykres graficzny przedstawiający najbardziej reprezentatywne dane raportu.
- Tabelę zbiorczą z wyliczonymi wskaźnikami raportu.
- Tabelę ze szczegółowymi danymi raportu.

Zapisywanie raportu

W celu zapisania utworzonego raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu wybierz żądany szablon raportu.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Zapisz**.

Zostanie uruchomiony Kreator zapisywania raportu. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu pracy kreatora, zostanie otwarty folder, w którym znajduje się zapisany plik raportu.

Tworzenie zadania dostarczania raportu

Raporty mogą być wysyłane za pośrednictwem poczty elektronicznej. Dostarczanie raportów w Kaspersky Security Center jest wykonywane przez zadanie dostarczania raportów.

W celu utworzenia zadania dostarczenia jednego raportu:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.
3. Na liście szablonów raportu wybierz żądany szablon raportu.
4. Z menu kontekstowego wybranego szablonu raportu wybierz **Dostarcz raporty**.

   Zostanie uruchomiony Kreator tworzenia zadania dostarczania raportu. Postępuj zgodnie z instrukcjami kreatora.

W celu utworzenia zadania dostarczania kilku raportów:

1. Z drzewa konsoli, w węźle z nazwą żądanego Serwera administracyjnego wybierz folder **Zadania**.
2. W obszarze roboczym folderu **Zadania** kliknij przycisk **Utwórz zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

   Nowo utworzone zadanie dostarczania raportów będzie wyświetlane w folderze **Zadania** drzewa konsoli.

Zadanie dostarczania raportu jest tworzone automatycznie, jeśli w trakcie instalacji Kaspersky Security Center określono ustawienia e-mail.

Krok 1. Wybieranie typu zadania

W oknie **Wybierz typ zadania**, na liście zadań jako typ zadania wybierz **Dostarcz raporty**.

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 2. Wybieranie typu raportu

W oknie **Wybierz typ raportu**, na liście szablonów tworzenia zadania wybierz typ raportu.

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 3. Działania podejmowane na raporcie

W oknie **Akcja stosowana wobec raportów** określ następujące ustawienia:

- Wysyłaj raporty przy użyciu e-mail

Jeśli ta opcja jest włączona, aplikacja wyśle wygenerowane raporty za pośrednictwem poczty elektronicznej.

Wysyłanie raportów w wiadomości e-mail można skonfigurować po kliknięciu odnośnika **Ustawienia powiadomień e-mail**. Odnośnik jest dostępny, jeśli ta opcja jest włączona.

Jeśli ta opcja jest wyłączona, aplikacja zapisze raporty w folderze wskazanym do ich przechowywania.

Domyślnie opcja ta jest wyłączona.

- Zapisuj raporty w folderze współdzielonym

  Jeśli ta opcja jest włączona, aplikacja zapisze raporty do folderu, który został określony w polu pod opcją do zaznaczenia. Aby zapisać raporty w folderze współdzielonym, określ ścieżkę UNC do folderu. W tym przypadku, w oknie **Wybieranie konta do uruchomienia zadania** musisz określić konto użytkownika i hasło dostępu do tego folderu.

  Jeśli ta opcja jest wyłączona, aplikacja nie zapisze raportów do folderu, a zamiast tego wyśle je za pośrednictwem poczty elektronicznej.

  Domyślnie opcja ta jest wyłączona.

- Nadpisz starsze raporty tego samego typu

  Jeśli ta opcja jest włączona, przy każdym uruchomieniu zadania nowy plik raportu nadpisze plik zapisany w folderze raportów przy poprzednim uruchomieniu zadania.

  Jeśli ta opcja jest wyłączona, pliki raportów nie będą nadpisywane. Nowy plik raportu jest przechowywany w folderze raportów przy każdym uruchomieniu zadania.

  To pole jest dostępne, jeśli zaznaczona jest opcja **Zapisz raport do folderu**.

  Domyślnie opcja ta jest wyłączona.

- Określ konto, które ma mieć dostęp do folderu współdzielonego

  Jeśli ta opcja jest włączona, możesz określić konto, z poziomu którego raport zostanie zapisany do folderu. Jeśli ścieżka UNC do folderu współdzielonego jest określona jako ustawienie **Zapisz raport w folderze** w oknie **Akcja stosowana wobec raportów**, musisz określić konto użytkownika i hasło dostępu do tego folderu.

  Jeśli ta opcja jest wyłączona, raport zostanie zapisany do folderu z poziomu konta Serwera administracyjnego.

  To pole jest dostępne, jeśli zaznaczona jest opcja **Zapisz raport do folderu**.

  Domyślnie opcja ta jest wyłączona.

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 4. Wybieranie konta do uruchamiania zadania

W oknie **Wybieranie konta do uruchomienia zadania** możesz określić, które konto ma być używane podczas uruchamiania zadania. Wybierz jedną z następujących opcji:

- Konto domyślne

  Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

  Domyślnie opcja ta jest zaznaczona.

- Określ konto

  Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

  - Konto

    Konto, z poziomu którego zadanie jest uruchamiane.

  - Hasło

    Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 5. Konfigurowanie terminarza zadania

W oknie **Konfiguruj terminarz zadania** możesz utworzyć terminarz uruchamiania zadania. Jeśli to konieczne, zdefiniuj następujące ustawienia:

- Zaplanowane uruchomienie:

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - Co N godzin

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

    Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

  - Co N dni

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

    Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

  - Co N tygodni

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

    Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

  - Co N minut

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po epidemii wirusa**

Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

- Ochrona antywirusowa stacji roboczych i serwerów plików
- Ochrona antywirusowa bram internetowych
- Ochrona antywirusowa serwerów pocztowych

Domyślnie, zaznaczone są wszystkie typy aplikacji.

Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

Domyślnie opcja ta jest włączona.

- Używaj automatycznie losowego opóźnienia dla uruchamiania zadań

Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

Krok 6. Definiowanie nazwy zadania

W oknie **Określ nazwę zadania** określ nazwę dla zadania, które tworzysz. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych (`"*<>?\:|`).

Kliknij **Dalej**, aby przejść do kolejnego kroku.

Krok 7. Kończenie tworzenia zadania

W oknie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**, aby zakończyć pracę kreatora.

Jeśli chcesz, żeby zadanie było uruchamiane zaraz po zakończeniu pracy kreatora, zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**.

Zarządzanie statystykami

Statystyki dotyczące stanu systemu ochrony i zarządzanych urządzeń są wyświetlane w panelach informacyjnych, które można dostosować. Statystyki są wyświetlane w obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Statystyki**. Zakładka zawiera kilka zakładek (stron) drugiego poziomu. Każda strona wyświetla panele informacyjne ze statystykami, a także odnośniki do nowości i innych materiałów z Kaspersky. Informacje statystyczne są wyświetlane na panelach informacyjnych jako tabela lub wykres (kołowy lub słupkowy). Dane w panelach informacyjnych są aktualizowane w trakcie działania aplikacji i odzwierciedlają bieżący stan aplikacji antywirusowej.

Możesz zmodyfikować zestaw zakładek drugiego poziomu na zakładce **Statystyki**, zmienić liczbę paneli informacyjnych na każdej zakładce oraz tryb wyświetlania danych w panelach informacyjnych.

*W celu dodania nowej zakładki drugiego poziomu z panelami informacyjnymi na zakładce **Statystyki**:*

1. Kliknij przycisk **Dostosuj widok** znajdujący się w prawym górnym rogu zakładki **Statystyki**.

   Zostanie otwarte okno właściwości statystyk. To okno zawiera listę zakładek, które są aktualnie wyświetlane na zakładce **Statystyki**. W tym oknie możesz zmienić kolejność wyświetlania stron na zakładce, dodać i usunąć strony, a także skonfigurować właściwości strony, klikając przycisk **Właściwości**.

2. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno właściwości nowej strony.

3. Skonfiguruj nową stronę:

   - W sekcji **Ogólny** określ nazwę strony.
   - W sekcji **Panele informacyjne** kliknij przycisk **Dodaj**, aby dodać panele informacyjne, które mają być wyświetlane na stronie.

     W sekcji **Panele informacyjne** kliknij przycisk **Właściwości**, aby skonfigurować właściwości dodanych paneli informacyjnych: nazwę, typ i wygląd wykresu na panelu oraz dane niezbędne do utworzenia wykresu.

4. Kliknij **OK**.

Strona z panelami informacyjnymi, które dodałeś, pojawi się na zakładce **Statystyki**. Kliknij ikonę ustawienia (⚙), aby natychmiast przejść do konfiguracji strony lub wybranego panelu informacyjnego na tej stronie.

Konfigurowanie powiadomień o zdarzeniach

Kaspersky Security Center umożliwia wybranie metody powiadamiania administratora o zdarzeniach występujących na urządzeniach klienckich oraz skonfigurowanie powiadomień:

- Poprzez e-mail. Po wystąpieniu zdarzenia, aplikacja wyśle powiadomienie na określone adresy e-mail. Możesz zmodyfikować treść powiadomienia.
- Za pośrednictwem wiadomości SMS. Po wystąpieniu zdarzenia, aplikacja wyśle powiadomienie na określone numery telefonu. Możesz skonfigurować wysyłanie powiadomień SMS poprzez bramkę pocztową.
- Poprzez uruchomienie pliku wykonywalnego. Po wystąpieniu zdarzenia na urządzeniu, na stacji roboczej administratora zostanie uruchomiony plik wykonywalny. Korzystając z pliku wykonywalnego, administrator może pobrać parametry dowolnego zdarzenia, które wystąpiło.

W celu skonfigurowania wysyłania powiadomień o zdarzeniach występujących na urządzeniach klienckich:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Kliknij odnośnik **Konfiguruj powiadomienia i eksportowanie zdarzeń** i z listy rozwijalnej wybierz wartość **Konfiguruj powiadomienia**.

   Spowoduje to otwarcie okna **Właściwości: Zdarzenia**.
4. W sekcji **Powiadamianie** wybierz metodę powiadamiania (poprzez e-mail, za pośrednictwem wiadomości SMS lub przez uruchomienie pliku wykonywalnego) i zdefiniuj ustawienia powiadomień:

   - **E-mail**

Zakładka **E-mail** umożliwia skonfigurowanie wysyłania powiadomień o zdarzeniach za pośrednictwem poczty elektronicznej.

W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami.

W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX**, możesz użyć kilku wpisów MX adresów IP dla tej samej nazwy DNS serwera SMTP. Ta sama nazwa DNS może posiadać kilka wpisów MX z różnymi wartościami priorytetu odbierania wiadomości e-mail. Serwer administracyjny spróbuje wysłać powiadomienia e-mail do serwera SMTP w kolejności rosnącej priorytetów wpisów MX. Domyślnie opcja ta jest wyłączona.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX** i nie włączysz korzystania z ustawień TLS, zalecane jest użycie ustawień DNSSEC na urządzeniu serwerowym jako dodatkowego środka ochrony wysyłania powiadomień e-mail.

Kliknij odnośnik **Ustawienia**, aby zdefiniować dodatkowe ustawienia powiadomień:

- Nazwa podmiotu (nazwa podmiotu wiadomości e-mail)
- Adres e-mail nadawcy
- Ustawienia uwierzytelniania ESMTP

Jeśli dla serwera SMTP włączono uwierzytelnianie ESMTP, do autoryzacji na serwerze SMTP należy określić konto.

- Ustawienia TLS dla serwera SMTP:
  - **Nie korzystaj z TLS**

    Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.
  - **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

    Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.
  - **Zawsze używaj TLS, sprawdź certyfikat serwera pod kątem ważności**

    Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź certyfikat serwera pod kątem ważności**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić ustawienia TLS dla serwera SMTP:

- Odszukaj plik certyfikatu serwera SMTP:

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

- Odszukaj plik certyfikatu klienta:

Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

- Certyfikat X-509:

Musisz określić plik z certyfikatem oraz plik z kluczem prywatnym. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po załadowaniu obu plików należy określić hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- Kontener pkcs12:

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia. Lista dodatkowych parametrów jest dostępna po kliknięciu przycisku, znajdującego się z prawej strony pola.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%”.

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy poprawnie skonfigurowałeś powiadomienia. Aplikacja powinna wysłać powiadomienie testowe na adresy e-mail, które określiłeś.

- SMS

Na zakładce **SMS** możesz skonfigurować wysyłanie powiadomień SMS o różnych zdarzeniach na telefon komórkowy. Wiadomości SMS są wysyłane poprzez bramkę pocztową.

W polu **Odbiorcy (adresy e-mail)** określ adres e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami. Powiadomienia będą dostarczane na numery telefonów skojarzone z określonymi adresami e-mail.

W polu **Serwery SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Kliknij odnośnik **Ustawienia**, aby zdefiniować dodatkowe ustawienia powiadomień:

- Nazwa podmiotu (nazwa podmiotu wiadomości e-mail)
- Adres e-mail nadawcy
- Ustawienia uwierzytelniania ESMTP

Jeśli to konieczne, jeśli dla serwera SMTP włączono uwierzytelnianie ESMTP, do autoryzacji na serwerze SMTP możesz określić konto.

- Ustawienia TLS dla serwera SMTP

Możesz wyłączyć korzystanie z TLS, użyć TLS, jeśli serwer SMTP obsługuje ten protokół lub możesz wymusić użycie tylko TLS. Jeśli zdecydujesz się używać tylko TLS, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Dodatkowo, jeśli wybierzesz używanie tylko TLS, możesz określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

- Odszukaj plik certyfikatu serwera SMTP

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Kaspersky Security Center. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może zawierać pustą wartość, jeśli klucz prywatny nie zostanie zakodowane. Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami o zdarzeniu, które aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia. Lista dodatkowych parametrów jest dostępna po kliknięciu przycisku, znajdującego się z prawej strony pola.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%”.

Kliknij odnośnik **Ustaw limit liczby powiadomień**, aby określić maksymalną liczbę powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy powiadomienia zostały skonfigurowane poprawnie. Aplikacja powinna wysłać powiadomienie testowe do określonych odbiorców.

- Plik wykonywalny do uruchomienia

Jeśli wybrana jest ta metoda powiadamiania, w polu wejściowym określ aplikację, która zostanie uruchomiona, gdy wystąpi zdarzenie.

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Przycisk **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie na wskazany adres e-mail.

5. W polu **Treść powiadomienia** wprowadź tekst, który aplikacja wyśle po wystąpieniu zdarzenia.

   Możesz użyć listy rozwijanej znajdującej się na prawo od pola tekstowego, aby dodać dodatkowe ustawienia ze szczegółami zdarzenia (na przykład: opis zdarzenia lub czas wystąpienia).

   Jeżeli tekst powiadomienia zawiera znak %, należy go określić dwukrotnie, aby umożliwić wysłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%".

6. Kliknij przycisk **Wyślij wiadomość testową**, aby sprawdzić, czy powiadomienia zostały skonfigurowane poprawnie.

   Aplikacja wysyła powiadomienie testowe do określonego użytkownika.

7. Kliknij **OK**, aby zachować zmiany.

Skonfigurowane ustawienia powiadamiania zostaną zastosowane do wszystkich zdarzeń występujących na urządzeniach klienckich.

Możesz zastąpić ustawienia powiadamiania dla pewnych zdarzeń w sekcji **Konfiguracja zdarzenia** ustawień Serwera administracyjnego, ustawień profilu lub ustawień aplikacji.

Tworzenie certyfikatu dla serwera SMTP

W celu utworzenia certyfikatu dla serwera SMTP:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Kliknij odnośnik **Konfiguruj powiadomienia i eksportowanie zdarzeń** i z listy rozwijalnej wybierz wartość **Konfiguruj powiadomienia**.

   Zostanie otwarte okno właściwości zdarzenia.

4. Na zakładce **E-mail** kliknij odnośnik **Ustawienia**, aby otworzyć okno **Ustawienia**.
5. W oknie **Ustawienia** kliknij odnośnik **Określ certyfikat**, aby otworzyć okno **Certyfikat do podpisu**.
6. W oknie **Certyfikat do podpisu** kliknij przycisk **Przeglądaj**.

   Zostanie otwarte okno **Certyfikat**.

7. Z listy rozwijalnej **Typ certyfikatu** wybierz typ certyfikatu - publiczny lub prywatny:

   - Jeśli wybrany jest certyfikat prywatny (**Kontener PKCS #12**), określ plik certyfikatu i hasło.

- Jeśli wybrany jest certyfikat publiczny (**Certyfikat X.509**):

  a. Określ plik klucza prywatnego (z rozszerzeniem *.prk lub *.pem).

  b. Określ hasło dla klucza prywatnego.

  c. Określ plik klucza publicznego (z rozszerzeniem *.cer).

8. Kliknij **OK**.

Zostanie utworzony certyfikat dla serwera SMTP.

Wybory zdarzeń

Informacje o zdarzeniach, które wystąpiły w trakcie działania Kaspersky Security Center i zarządzanych aplikacji, są zapisywane w bazie danych Serwera Administracyjnego i w dzienniku systemu Microsoft Windows. Możesz przejrzeć informacje z bazy danych Serwera administracyjnego w obszarze roboczym węzła **Serwer Administracyjny**, na zakładce **Zdarzenia**.

Informacje na zakładce **Zdarzenia** są przedstawione pod postacią listy wyborów zdarzeń. Każdy wybór zawiera tylko zdarzenia określonego typu. Na przykład, wybór „Stan urządzenia jest Krytyczny" zawiera tylko wpisy dotyczące zmiany stanów urządzeń na „Krytyczny". Po zainstalowaniu aplikacji, zakładka **Zdarzenia** posiada kilka standardowych wyborów zdarzeń. Możesz tworzyć dodatkowe (niestandardowe) wybory zdarzeń lub eksportować informacje o zdarzeniach do pliku.

Przeglądanie wyboru zdarzeń

W celu przejrzenia wyboru zdarzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.

3. Z listy rozwijalnej **Wybory zdarzeń** wybierz żądany wybór zdarzeń.

   Jeśli chcesz, żeby zdarzenia z tego wyboru były cały czas wyświetlane w obszarze roboczym, kliknij ikonę gwiazdki (☆) znajdującą się obok wyboru.

   Obszar roboczy będzie wyświetlał listę zdarzeń wybranego typu, przechowywanych na Serwerze administracyjnym.

Informacje przedstawione na liście zdarzeń mogą być sortowane (rosnąco lub malejąco) według dowolnej kolumny.

Dostosowywanie wyboru zdarzeń

W celu dostosowania wyboru zdarzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.

3. Na zakładce **Zdarzenia** otwórz żądany wybór zdarzeń.

4. Kliknij przycisk **Właściwości wyboru**.

W otwartym oknie właściwości wyboru zdarzeń możesz skonfigurować wybór zdarzeń.

Tworzenie kryterium wyboru zdarzenia

W celu utworzenia wyboru zdarzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.

3. Kliknij przycisk **Utwórz wybór**.

4. W oknie **Nowy wybór zdarzeń**, które zostanie otwarte, wprowadź nazwę nowego wyboru i kliknij **OK**.

Na liście rozwijalnej **Wybory zdarzeń** zostanie utworzony wybór pod nazwą, którą określiłeś.

Domyślnie utworzone kryterium wyboru zdarzeń zawiera wszystkie zdarzenia przechowywane na Serwerze administracyjnym. Aby wybór wyświetlał tylko żądane zdarzenia, należy go skonfigurować.

Eksportowanie wyboru zdarzeń do pliku tekstowego

W celu wyeksportowania wyboru zdarzeń do pliku tekstowego:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.

3. Kliknij przycisk **Import/Eksport**.

4. Z listy rozwijalnej wybierz **Eksportuj zdarzenia do pliku**.

Zostanie uruchomiony Kreator eksportu zdarzeń. Postępuj zgodnie z instrukcjami kreatora.

Usuwanie zdarzeń z wyboru

W celu usunięcia zdarzeń z wyboru:

1. Z drzewa konsoli wybierz węzeł z nazwą odpowiedniego Serwera administracyjnego.

2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.

3. Zaznacz zdarzenia, które chcesz usunąć, używając myszy bądź klawisza **Shift** lub **Ctrl**.

4. Usuń zaznaczone zdarzenia w jeden z następujących sposobów:

- Wybierając **Usuń** z menu kontekstowego dowolnego z wybranych zdarzeń.

  Jeżeli z menu kontekstowego wybrałeś element **Usuń wszystkie**, wszystkie wyświetlone zdarzenia zostaną usunięte z wyboru, bez względu na to, które zaznaczyłeś.

- Klikając odnośnik **Usuń zdarzenie** (jeśli wybrałeś jedno zdarzenie) lub **Usuń zdarzenia** (jeśli wybrałeś kilka zdarzeń) w oknie z informacjami dla tych zdarzeń.

Wybrane zdarzenia zostaną usunięte.

Dodawanie aplikacji do wykluczeń na żądanie użytkownika

Jeśli otrzymasz żądania użytkownika dotyczące odblokowania błędnie zablokowanych aplikacji, możesz utworzyć wykluczenie z reguł ochrony adaptacyjnej dla tych aplikacji. W konsekwencji aplikacje nie będą już blokowane na urządzeniach użytkowników. Możesz śledzić liczbę żądań użytkownika na zakładce **Monitorowanie** Serwera administracyjnego.

W celu dodania aplikacji zablokowanych przez Kaspersky Endpoint Security do wykluczeń według żądań użytkownika:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. W obszarze roboczym węzła wybierz zakładkę **Zdarzenia**.
3. Z listy rozwijalnej **Wybory zdarzeń** wybierz **Żądania użytkownika**.
4. Kliknij prawym klawiszem myszy żądanie użytkownika (lub kilka żądań użytkownika) zawierające aplikacje, które chcesz dodać do wykluczeń, a następnie wybierz **Dodaj wykluczenie**.

   Zostanie uruchomiony kreator Dodawania wykluczenia. Postępuj zgodnie z jego instrukcjami.

Wybrane aplikacje zostaną wykluczone z listy **Wywoływanie reguł w trybie Inteligentne uczenie się** (pod węzłem **Repozytoria** w drzewie konsoli) po kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym i nie pojawi się już więcej na liście.

Wybory urządzeń

Informacje o stanie urządzeń są wyświetlane w folderze **Wybory urządzeń** drzewa konsoli.

Informacje w folderze **Wybory urządzeń** są wyświetlane jako lista wyborów urządzeń. Każdy wybór zawiera urządzenia, które spełniają określone warunki. Na przykład, wybór **Urządzenia ze stanem Krytyczny** zawiera tylko urządzenia posiadające stan *Krytyczny*. Po zainstalowaniu aplikacji, folder **Wybory urządzeń** posiada kilka standardowych wyborów. Możesz tworzyć dodatkowe (niestandardowe) wybory urządzeń, eksportować ustawienia wyboru do pliku lub tworzyć wybory zgodnie z ustawieniami zaimportowanymi z innego pliku.

Wyświetlanie wyboru urządzeń

W celu wyświetlenia wyboru urządzeń:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.

2. W obszarze roboczym folderu, z listy **Wybrane urządzenia** wybierz odpowiedni wybór urządzeń.
3. Kliknij przycisk **Uruchom wybrane**.
4. Kliknij zakładkę **Wyniki wyborów**.

W obszarze roboczym zostanie wyświetlona lista urządzeń, które spełniają kryteria wyboru.

Informacje przedstawione na liście urządzeń mogą być sortowane (rosnąco lub malejąco) według dowolnej kolumny.

Konfigurowanie kryteriów wyboru urządzeń

W celu skonfigurowania kryteriów wyboru urządzeń:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.
2. W obszarze roboczy kliknij zakładkę **Wybór**, a następnie kliknij odpowiedni wybór urządzeń na liście wyborów użytkownika.
3. Kliknij przycisk **Właściwości wyboru**.
4. W otwartym oknie właściwości określ następujące ustawienia:
   - Ogólne właściwości wyboru.
   - Warunki, jakie muszą zostać spełnione do uwzględnienia urządzeń w tym wyborze. Możesz skonfigurować warunki po wybraniu nazwy warunku i kliknięciu przycisku **Właściwości**.
   - Ustawienia zabezpieczeń.
5. Kliknij **OK**.

   Ustawienia zostaną zastosowane i zapisane.

Poniżej znajdują się opisy warunków przydzielania urządzeń do wyboru. Warunki są łączone przy użyciu operatora logicznego LUB: Wybór będzie zawierał urządzenia odpowiadające przynajmniej jednemu z wymienionych warunków.

Ogólny

W sekcji **Ogólny** możesz zmienić nazwę warunku wyboru oraz określić, czy ten warunek ma być odwrócony:

Odwróć warunek wyboru

Jeśli ta opcja jest włączona, określony warunek wyboru zostanie odwrócony. Wybór będzie zawierał wszystkie urządzenia, które nie spełniają warunku.

Domyślnie opcja ta jest wyłączona.

Sieć

W sekcji **Sieć** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich danymi sieciowymi:

- **Nazwa urządzenia lub adres IP**

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- **Domena Windows**

  Wyświetla wszystkie urządzenia znajdujące się w określonej domenie Windows.

- **Grupa administracyjna**

  Wyświetla urządzenia znajdujące się w określonej grupie administracyjnej.

- **Opis**

Tekst wyświetlany w oknie właściwości urządzenia: pole **Opis** sekcji **Ogólny**.

W celu opisania tekstu w polu **Opis** możesz użyć następujących znaków:

- W słowie:
  - *****. Zastępuje dowolny wiersz dowolną liczbą znaków.

    Na przykład:

    Aby opisać słowa **Serwer** lub **Serwera**, możesz wpisać **Serwer***.
  - **?.** Zastępuje dowolny pojedynczy znak.

    Na przykład:

    Aby opisać słowa **Okno** lub **Okna**, możesz wpisać **Okn?**.

    Gwiazdka (*****) lub znak zapytania (**?**) nie mogą być używane jako pierwsze symbole wyszukiwanego słowa.
- W celu wyszukania kilku słów użyj:
  - Spacji. Wyświetla wszystkie urządzenia, których opisy zawierają dowolne z wymienionych słów.

    Na przykład:

    Aby odszukać frazę zawierającą słowa **Podrzędny** lub **Wirtualny**, wprowadź **Podrzędny Wirtualny** w tekście wyszukiwania.
  - **+**. Jeśli przed wyrazem wpisano znak "+", wszystkie wyniki wyszukiwania będą zawierać ten wyraz.

    Na przykład:

    Aby odszukać frazę zawierającą zarówno **Podrzędny**, jak i **Wirtualny**, wprowadź **+Podrzędny+Wirtualny**.
  - **-**. Jeśli przed wyrazem wpisano znak "-", żaden z wyników wyszukiwania nie będzie zawierać tego wyrazu.

    Na przykład:

    Aby odszukać frazę zawierającą **Podrzędny** i nie zawierającą **Wirtualny**, wprowadź **+Podrzędny-Wirtualny**.
  - **"<jakikolwiek tekst>"**. Tekst w cudzysłowach musi znajdować się w tekście.

    Na przykład:

    Aby odszukać frazę zawierającą kombinację słów **Podrzędny Serwer**, wprowadź **„Podrzędny Serwer"** w tekście wyszukiwania.

- Zakres IP

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

Znaczniki

W sekcji **Znaczniki** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o słowa kluczowe (znaczniki), które wcześniej zostały dodane do opisów zarządzanych urządzeń:

- **Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny**

  Jeśli ta opcja jest włączona, w wynikach wyszukiwania będą wyświetlane urządzenia z opisami, które zawierają przynajmniej jeden z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, w wynikach wyszukiwania będą wyświetlane tylko urządzeni z opisami, które zawierają wszystkie wybrane znaczniki.

  Domyślnie opcja ta jest wyłączona.

- **Musi zawierać znacznik**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy zawierają wybrany znacznik. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

  Domyślnie opcja ta jest zaznaczona.

- **Nie może zawierać znacznika**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy nie zawierają wybranego znacznika. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

Active Directory

W sekcji **Active Directory** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich dane Active Directory:

- **Urządzenie znajduje się w jednostce organizacyjnej Active Directory**

  Jeśli ta opcja jest włączona, wybór będzie zawierał urządzenia z jednostki Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

- **Uwzględnij podrzędne jednostki organizacyjne**

  Jeśli ta opcja jest włączona, wybór zawiera urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej Active Directory.

  Domyślnie opcja ta jest wyłączona.

- **Urządzenie należy do grupy Active Directory**

  Jeśli ta opcja jest włączona, wybór będzie zawierał komputery z grupy Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

Aktywność sieciowa

W sekcji **Aktywność sieciowa** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich aktywnością sieciową:

- Urządzenie jest punktem dystrybucji

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór zawiera urządzenia pełniące role punktów dystrybucji.
  - **Nie**. Urządzenia pełniące role punktów dystrybucji nie będą uwzględniane w wyborze.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Nie odłączaj od Serwera administracyjnego

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Włączono**. Wybór będzie zawierał urządzenia, na których zaznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Wyłączono**. Wybór będzie zawierał urządzenia, na których odznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Przełączanie profilu połączenia

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór będzie zawierał urządzenia, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie**. Wybór nie będzie zawierał urządzeń, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Ostatnie połączenie z Serwerem administracyjnym

  To pole ustawia kryterium wyszukiwania urządzeń według godziny ostatniego połączenia z Serwerem administracyjnym.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego zostało nawiązane ostatnie połączenie pomiędzy Agentem sieciowym zainstalowanym na urządzeniu klienckim a Serwerem administracyjnym. Wybór będzie zawierał urządzenia mieszczące się w określonym przedziale czasu.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- Nowe urządzenia odnalezione podczas skanowania sieci

Wyszukiwanie nowych urządzeń, które zostały wykryte podczas przeszukiwania sieci w przeciągu kilku ostatnich dni.

Jeśli ta opcja jest włączona, wybór będzie zawierał nowe urządzenia wykryte podczas wykrywania urządzeń w czasie określonym w polu **Okres wykrywania (dni)**.

Jeśli ta opcja jest wyłączona, wybór będzie zawierał wszystkie urządzenia wykryte podczas wykrywania urządzeń.

Domyślnie opcja ta jest wyłączona.

- **Dostępność urządzenia**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie widoczne w sieci.
  - **Nie**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie niewidoczne w sieci.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

Aplikacja

W sekcji **Aplikacja** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o wybraną zarządzaną aplikację:

- **Nazwa aplikacji**

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji Kaspersky.

  Lista zawiera tylko nazwy aplikacji z wtyczkami administracyjnymi zainstalowanych na stacji roboczej administratora.

  Jeśli żadna aplikacja nie została wybrana, kryterium nie będzie stosowane.

- **Wersja aplikacji**

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według numeru wersji aplikacji Kaspersky.

  Jeśli żaden numer wersji nie został określony, kryterium nie będzie stosowane.

- **Nazwa aktualizacji krytycznej**

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji lub numeru pakietu aktualizacyjnego.

  Jeśli pole będzie puste, kryterium nie będzie stosowane.

- **Ostatnia aktualizacja modułów**

Ta opcja może zostać użyta do ustawienia kryterium wyszukiwania urządzeń według godziny ostatniej aktualizacji modułów aplikacji zainstalowanych na tych urządzeniach.

Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego została wykonana ostatnia aktualizacja modułów aplikacji zainstalowanych na tych urządzeniach.

Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

Domyślnie pole to nie jest zaznaczone.

- Urządzenie jest zarządzane przez Kaspersky Security Center

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić urządzenia zarządzane poprzez Kaspersky Security Center:

  - **Tak**. Aplikacja uwzględni w wyborze urządzenia zarządzane poprzez Kaspersky Security Center.
  - **Nie**. Aplikacja uwzględni w wyborze urządzenia, jeśli nie są one zarządzane przez Kaspersky Security Center.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Aplikacja zabezpieczająca jest zainstalowana

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą:

  - **Tak**. Aplikacja uwzględni w wyborze wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą.
  - **Nie**. Aplikacja uwzględni w wyborze wszystkie urządzenia bez zainstalowanej aplikacji zabezpieczającej.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

System operacyjny

W sekcji **System operacyjny** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z typem systemu operacyjnego.

- Wersja systemu operacyjnego

  Jeśli pole jest zaznaczone, możesz wybrać system operacyjny z listy. Urządzenia, na których zainstalowany jest określony system operacyjny, są uwzględniane w wynikach wyszukiwania.

- Typ systemu operacyjnego (bity)

  Z listy rozwijalnej możesz wybrać architekturę swojego systemu operacyjnego, która określi sposób stosowania reguły przenoszenia do urządzenia (**Nieznany**, **x86**, **AMD64**, or **IA64**). Domyślnie, na liście nie wybrano żadnej opcji i tym samym nie zdefiniowano architektury systemu operacyjnego.

- Wersja dodatku Service Pack systemu operacyjnego

W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- Kompilacja systemu operacyjnego

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Numer kompilacji systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować wyszukiwanie wszystkich numerów kompilacji, za wyjątkiem określonego.

- ID wersji systemu operacyjnego

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Identyfikator wydania systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy identyfikator wydania. Możesz także skonfigurować wyszukiwanie wszystkich numerów identyfikatorów wydania, za wyjątkiem określonego.

Stan urządzenia

W sekcji **Stan urządzenia** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o opis stanu urządzeń z zarządzanej aplikacji:

- Stan urządzenia

  Lista rozwijalna, z której możesz wybrać jeden ze stanów urządzenia: *OK*, *Krytyczny*, or *Ostrzeżenie*.

- Opis stanu urządzenia

  W tym polu możesz zaznaczyć pola obok warunków, które, jeśli są spełnione, spowodują przypisanie do urządzenia jednego z następujących stanów: *OK, Krytyczny*, or *Ostrzeżenie*.

- Stan urządzenia zdefiniowany przez aplikację

  Lista rozwijalna, z której możesz wybrać stan ochrony w czasie rzeczywistym. Urządzenia z określonymi stanami ochrony w czasie rzeczywistym są uwzględniane w wyborze.

Składniki ochrony

W sekcji **Składniki ochrony** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich stan ochrony:

- **Data opublikowania baz danych**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według daty opublikowania antywirusowej bazy danych. W polach do wprowadzania danych możesz określić przedział czasu, na podstawie którego wykonywane jest wyszukiwanie.

  Domyślnie opcja ta jest wyłączona.

- **Ostatnie skanowanie**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według czasu ostatniego skanowania w poszukiwaniu złośliwego oprogramowania. W polach wejściowych możesz określić przedział czasu, w trakcie którego zostało wykonane ostatnie skanowanie w poszukiwaniu złośliwego oprogramowania.

  Domyślnie opcja ta jest wyłączona.

- **Całkowita liczba wykrytych zagrożeń**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wykrytych wirusów. W polach wejściowych możesz określić niższe i wyższe wartości progowe liczby wykrytych wirusów.

  Domyślnie opcja ta jest wyłączona.

Rejestr aplikacji

W sekcji **Rejestr aplikacji** możesz skonfigurować kryteria wyszukiwania urządzeń na podstawie aplikacji na nich zainstalowanych:

- **Nazwa aplikacji**

  Lista rozwijalna, z której możesz wybrać aplikację. Urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Wersja aplikacji**

  Pole, w którym możesz określić wersję wybranej aplikacji.

- **Producent**

  Lista rozwijalna, z której możesz wybrać producenta aplikacji zainstalowanej na urządzeniu.

- **Stan aplikacji**

  Lista rozwijalna, z której możesz wybrać stan aplikacji (*Zainstalowana*, *Nie zainstalowana*). Urządzenia, na których określona aplikacja została zainstalowana lub nie została zainstalowana, w zależności od wybranego stanu, zostaną uwzględnione w wyborze.

- **Wyszukaj według aktualizacji**

Jeśli ta opcja jest włączona, wyszukiwanie będzie się odbywać z użyciem szczegółów aktualizacji dla aplikacji zainstalowanych na odpowiednich urządzeniach. Po zaznaczeniu pola, pola **Nazwa aplikacji**, **Wersja aplikacji** i **Stan aplikacji** zostaną zmienione na **Nazwa aktualizacji**, **Wersja aktualizacji** i **Stan**.

Domyślnie opcja ta jest wyłączona.

- Nazwa niekompatybilnej aplikacji zabezpieczającej

  Lista rozwijalna, z której możesz wybrać aplikacje zabezpieczające firm trzecich. Podczas wyszukiwania, urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- Znacznik aplikacji

  Z listy rozwijalnej możesz wybrać znacznik aplikacji. Wszystkie urządzenia, na których są zainstalowane aplikacje z wybranym znacznikiem w opisie, zostają uwzględnione w wyborze urządzeń.

- Zastosuj do urządzeń bez określonych znaczników

  Jeśli ta opcja jest włączona, wybór obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

  Domyślnie opcja ta jest wyłączona.

Rejestr sprzętu

W sekcji **Rejestr sprzętu** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o sprzęt na nich zainstalowany:

- Urządzenie

  Z listy rozwijalnej możesz wybrać typ jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- Producent

  Z listy rozwijalnej możesz wybrać nazwę producenta jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- Nazwa urządzenia

  Nazwa urządzenia w sieci Windows. Urządzenie z określoną nazwą zostanie uwzględniony w wyborze.

- Opis

Opis urządzenia lub sprzętu. Urządzenia z opisem określonym w tym polu zostaną uwzględnione w wyborze.

Opis urządzenia w dowolnym formacie może zostać wprowadzony w oknie właściwości tego urządzenia. Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent urządzenia**

  Nazwa producenta urządzenia. Urządzenia, które zostały wyprodukowane przez producenta określonego w tym polu, zostaną uwzględnione w wyborze.

  Nazwę producenta można wprowadzić w oknie właściwości urządzenia.

- **Numer seryjny**

  Cały sprzęt o numerze seryjnym określonym w tym polu zostanie uwzględniony w wyborze.

- **Numer ewidencyjny**

  Sprzęt o numerze inwentarzowym podanym w tym polu zostanie uwzględniony w wyborze.

- **Użytkownik**

  Cały sprzęt użytkownika określonego w tym polu zostanie uwzględniony w wyborze.

- **Lokalizacja**

  Lokalizacja urządzenia lub sprzętu (na przykład: w kwaterze głównej lub w oddziale firmy). Komputery lub inne urządzenia zainstalowane w lokalizacji określonej w tym polu zostaną uwzględnione w wyborze.

  Możesz opisać lokalizację urządzenia w dowolnym formacie w oknie właściwości tego urządzenia.

- **Częstotliwość procesora, w MHz**

  Zakres częstotliwości procesora. Urządzenia z procesorami odpowiadającymi zakresowi częstotliwości określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- **Wirtualne rdzenie procesora**

  Zakres liczby wirtualnych rdzeni w procesorze. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- **Pojemność dysku twardego, w GB**

  Zakres wartości rozmiaru dysku twardego urządzenia. Urządzenia z dyskami twardymi odpowiadającymi zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

- **Rozmiar pamięci RAM, w MB**

Zakres wartości rozmiaru pamięci RAM urządzenia. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

Maszyny wirtualne

W sekcji **Maszyny wirtualne** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w zależności od tego, czy są to maszyny wirtualne lub czy są one częścią infrastruktury pulpitu wirtualnego (VDI):

- Jest maszyną wirtualną

  Z listy rozwijalnej możesz wybrać następujące opcje:
  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Wyszukuje urządzenia, które są maszynami wirtualnymi.

- Typ maszyny wirtualnej

  Z listy rozwijalnej możesz wybrać producenta maszyny wirtualnej.

  Ta lista rozwijalna jest dostępna, jeśli wartość **Tak** lub **Nieważne** została wybrana na liście rozwijalnej **Jest maszyną wirtualną**.

- Część Virtual Desktop Infrastructure

  Z listy rozwijalnej możesz wybrać następujące opcje:
  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są częścią Virtual Desktop Infrastructure.
  - **Tak**. Wyszukuje urządzenia, które są częścią Virtual Desktop Infrastructure (VDI).

Luki oraz aktualizacje

W sekcji **Luki oraz aktualizacje** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich źródłem Windows Update:

WUA został przełączony na Serwer administracyjny

Z listy rozwijalnej można wybrać jedną z następujących opcji wyszukiwania:
- **Tak**. Jeśli wybrano tę opcję, wyniki wyszukiwania będą uwzględniać urządzenia, które uzyskały aktualizacje poprzez Windows Update z Serwera administracyjnego.
- **Nie**. Jeśli wybrano tę opcję, wyniki będą uwzględniać urządzenia, które uzyskały aktualizacje za pośrednictwem Windows Update z innych źródeł.

Użytkownicy

W sekcji **Użytkownicy** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze według kont użytkowników, którzy logowali się do systemu operacyjnego.

- Ostatni użytkownik zalogowany do systemu

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik ostatnio logował się do systemu.

- Użytkownik zalogowany do systemu co najmniej raz

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik przynajmniej raz logował się do systemu.

Problemy mające wpływ na stan zarządzanych aplikacji

W sekcji **Problemy mające wpływ na stan zarządzanych aplikacji** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze według listy możliwych problemów wykrytych przez zarządzaną aplikację. Jeśli przynajmniej jeden problem, który wybrałeś, istnieje na urządzeniu, urządzenie zostanie uwzględnione w wyborze. Jeśli wybierzesz problem wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego problemu na wszystkich listach.

Opis stanu urządzenia

Możesz zaznaczyć opcje dla opisów stanów z zarządzanej aplikacji. Po odebraniu tych stanów, urządzenia zostaną uwzględnione w wyborze. Jeśli wybierzesz stan wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego stanu na wszystkich listach.

Stan komponentów w zarządzanych aplikacjach

W sekcji **Stan komponentów w zarządzanych aplikacjach** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o stany komponentów w zarządzanych aplikacjach:

- Stan ochrony przed wyciekiem danych

  Wyszukiwanie urządzeń według stanu Ochrona przed wyciekaniem danych (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymano, Uruchomione, Niepowodzenie*).

- Stan ochrony serwerów współpracy

  Wyszukiwanie urządzeń według stanu ochrony serwerów współpracy (*Brak danych z urządzenia*, *Zatrzymana*, *Uruchamianie, Wstrzymano*, *Uruchomione*, *Niepowodzenie*).

- Stan ochrony antywirusowej serwerów pocztowych

  Wyszukiwanie urządzeń według stanu ochrony dla serwerów pocztowych (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymano, Uruchomione, Niepowodzenie*).

- **Stan czujnika Endpoint Sensor**

  Wyszukiwanie urządzeń według stanu komponentu Endpoint Sensor (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymano, Uruchomione, Niepowodzenie*).

Szyfrowanie

Algorytm szyfrowania

Algorytm blokowego szyfru symetrycznego AES (Advanced Encryption Standard). Z listy rozwijalnej możesz wybrać długość klucza szyfrowania (56-bitowy, 128-bitowy, 192-bitowy lub 256-bitowy).

Dostępne wartości: *AES56*, *AES128*, *AES192* i *AES256*.

Segmenty chmury

W sekcji **Segmenty chmury** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich odpowiednie segmenty chmury:

- **Urządzenie znajduje się w segmencie chmury**

  Jeśli ta opcja jest włączona, możesz kliknąć przycisk **Przeglądaj**, aby określić przeszukiwany segment.

  Jeśli włączono także opcję **Włączając obiekty potomne**, wyszukiwanie jest uruchamiane na wszystkich obiektach potomnych określonego segmentu.

  Wyniki wyszukiwania zawierają tylko urządzenia z wybranego segmentu.

- **Urządzenie wykryte przy pomocy API**

  Z listy rozwijalnej możesz wybrać, czy urządzenie jest wykrywane przez narzędzia API:

  - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.
  - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.
  - **Google Cloud.** Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku Google Cloud.
  - **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale nie może zostać wykryte przy użyciu API.
  - **Brak wartości**. Warunek nie ma zastosowania.

Składniki aplikacji

Ta sekcja zawiera listę komponentów tych aplikacji, które posiadają odpowiednie wtyczki administracyjne, zainstalowane w Konsoli administracyjnej.

W sekcji **Składniki aplikacji** możesz określić kryteria uwzględniania urządzeń w wyborze zgodnie ze stanami i numerami wersji komponentów, które odpowiadają wybranej aplikacji:

- **Stan**

  Wyszukiwanie urządzeń zgodnie ze stanem komponentu wysłanym przez aplikację do Serwera administracyjnego. Możesz wybrać jeden z następujących stanów: *Brak danych z urządzenia*, *Zatrzymane*, *Uruchamianie*, *Wstrzymane*, *Uruchomione*, *Błąd* lub *Nie zainstalowano*. Jeśli wybrany komponent aplikacji zainstalowanej na zarządzanym urządzeniu posiada określony stan, urządzenie jest uwzględniane w wyborze urządzeń.

  Stany wysłane przez aplikacje:

  - *Uruchamianie*—komponent jest właśnie w procesie inicjalizacji.
  - *Uruchomione*—komponent jest włączony i działa poprawnie.
  - *Wstrzymane*—komponent został zawieszony, na przykład, po wstrzymaniu przez użytkownika ochrony w zarządzanej aplikacji.
  - *Błąd*—podczas działania komponentu wystąpił błąd.
  - *Zatrzymane*—komponent jest wyłączony i nie działa w tym momencie.
  - *Nie zainstalowano*—użytkownik nie wybrał komponentu do zainstalowania podczas konfigurowania niestandardowej instalacji aplikacji.

  W przeciwieństwie do pozostałych stanów, stan *Brak danych z urządzenia* nie jest wysyłany przez aplikacje. Ta opcja pokazuje, że aplikacje nie posiadają informacji o wybranym stanie komponentu. Na przykład, to może mieć miejsce, gdy wybrany komponent nie należy do żadnej z aplikacji zainstalowanych na urządzeniu lub gdy urządzenie jest wyłączone.

- **Wersja**

  Wyszukiwanie urządzeń zgodnie z numerem wersji komponentu, który wybierasz na liście. Możesz wpisać numer wersji, na przykład `3.4.1.0`, a następnie określić, czy wybrany komponent musi posiadać równą, wcześniejszą lub nowszą wersję. Możesz także skonfigurować wyszukiwanie wszystkich wersji, za wyjątkiem określonej.

Eksportowanie ustawień wyboru urządzeń do pliku

W celu wyeksportowania ustawień wyboru urządzenia do pliku tekstowego:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.
2. W obszarze roboczym, na zakładce **Wybór** kliknij odpowiedni wybór urządzeń na liście wyborów użytkownika.

Ustawienia mogą być eksportowane tylko z wyborów urządzeń utworzonych przez użytkownika.

3. Kliknij przycisk **Uruchom wybrane**.

4. Na zakładce **Wyniki wyborów** kliknij przycisk **Eksportuj ustawienia**.

5. W oknie **Zapisz jako**, które zostało otwarte, określ nazwę wyboru pliku eksportowania ustawień, wybierz folder, w którym zostanie zapisany, i kliknij przycisk **Zapisz**.

Ustawienia wyboru urządzenia zostaną zapisane do określonego pliku.

Tworzenie kryteriów wyboru urządzeń

W celu utworzenia kryterium wyboru urządzeń:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.

2. W obszarze roboczym folderu kliknij przycisk **Zaawansowane** i wybierz z listy rozwijalnej **Utwórz wybór**.

3. W oknie **Nowy wybór urządzeń**, które zostanie otwarte, wprowadź nazwę nowego wyboru i kliknij **OK**.

Nowy folder z podaną nazwą pojawi się w drzewie konsoli, w folderze **Wybory urządzeń**. Domyślnie nowy wybór urządzeń zawiera wszystkie urządzenia wchodzące w skład grup administracyjnych na Serwerze administracyjnym, na którym utworzono wybór. Aby wybór wyświetlał tylko żądane urządzenia, skonfiguruj wybór poprzez kliknięcie przycisku **Właściwości wyboru**.

Tworzenie wyboru urządzeń zgodnie z zaimportowanymi ustawieniami

W celu utworzenia wyboru urządzeń zgodnie z zaimportowanymi ustawieniami:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.

2. W obszarze roboczym folderu kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz **Importuj wybór z pliku**.

3. W oknie, które zostanie otwarte, określ ścieżkę dostępu do pliku, z którego chcesz zaimportować ustawienia wyboru. Kliknij przycisk **Otwórz**.

Wpis **Nowy wybór** jest tworzony w folderze **Wybory urządzeń**. Ustawienia nowego wyboru są importowane z określonego pliku.

Jeżeli w folderze **Wybory urządzeń** istnieje już wybór o nazwie **Nowy wybór**, do nazwy tworzonego wyboru zostanie dodany przyrostek numeryczny **(<kolejny numer seryjny>)**, na przykład: **(1)**, **(2)**.

Usuwanie urządzeń z grup administracyjnych w wyborze

Podczas pracy z wyborami urządzeń możesz usunąć urządzenia z grup administracyjnych bezpośrednio w tym wyborze, bez przełączania do grup administracyjnych, z których te urządzenia mają być usunięte.

W celu usunięcia urządzeń z grup administracyjnych:

1. Z drzewa konsoli wybierz folder **Wybory urządzeń**.
2. Zaznacz urządzenia, które chcesz usunąć, używając klawisza **Shift** lub **Ctrl**.
3. Usuń zaznaczone urządzenia z grup administracyjnych w jeden z następujących sposobów:
   - Z menu kontekstowego jednego z zaznaczonych urządzeń wybierz **Usuń**.
   - Kliknij przycisk **Wykonaj akcję** i z listy rozwijalnej wybierz wartość **Usuń z grupy**

Wybrane urządzenia zostaną usunięte z odpowiednich grup administracyjnych.

Monitorowanie instalacji i dezinstalacji aplikacji

Możesz monitorować instalację lub dezinstalację określonych aplikacji na zarządzanych urządzeniach (na przykład, określonej przeglądarki). Aby użyć tej funkcji, możesz dodać aplikacje z Rejestru aplikacji do listy monitorowanych aplikacji. Jeśli monitorowana aplikacja jest instalowana lub dezinstalowana, Agent sieciowy publikuje odpowiednie zdarzenia: **Monitorowana aplikacja została zainstalowana** lub **Monitorowana aplikacja została odinstalowana**. Możesz monitorować te zdarzenia, korzystając z, na przykład, wyborów zdarzeń lub raportów.

Możesz monitorować te zdarzenia tylko wtedy, gdy są przechowywane w bazie danych Serwera administracyjnego.

W celu dodania aplikacji do listy monitorowanych aplikacji:

1. W folderze **Zaawansowane** → **Zarządzanie aplikacjami** w drzewie konsoli wybierz podfolder **Rejestr aplikacji**.
2. Nad listą aplikacji, która jest wyświetlana, kliknij przycisk **Pokaż okno właściwości rejestru aplikacji**.
3. W wyświetlonym oknie **Monitorowane aplikacje** kliknij przycisk **Dodaj**.
4. W wyświetlonym oknie **Wybierz nazwę aplikacji** wybierz aplikacje z Rejestru aplikacji, której instalację lub dezinstalację chcesz monitorować.
5. W oknie **Wybierz nazwę aplikacji** kliknij przycisk **OK**.

Po skonfigurowaniu listy monitorowanych aplikacji i zainstalowaniu lub odinstalowaniu zarządzanych urządzeń w swojej organizacji, możesz monitorować odpowiednie zdarzenia, na przykład, korzystać z wyboru zdarzeń Ostatnie zdarzenia.

Typy zdarzeń

Każdy komponent Kaspersky Security Center posiada swój zestaw typów zdarzeń. Ta sekcja zawiera listy typów zdarzeń, które wystąpiły w trakcie działania Serwera administracyjnego Kaspersky Security Center, Agenta sieciowego, serwera iOS MDM oraz serwera urządzeń mobilnych Exchange. Typy zdarzeń, które występują w aplikacjach Kaspersky, nie zostały wymienione w tej sekcji.

Struktura danych opisu typu zdarzeń

Dla każdego typu zdarzenia dostarczone są następujące elementy: wyświetlana nazwa, identyfikator (ID), kod alfabetyczny, opis oraz domyślny czas przechowywania.

- **Nazwa wyświetlanego typu zdarzenia**. Ten tekst jest wyświetlany w Kaspersky Security Center, gdy konfigurujesz zdarzenia oraz podczas występowania zdarzeń.
- **ID typu zdarzenia**. Ten kod numeryczny jest używany, gdy przetwarzasz zdarzenia przy użyciu narzędzi firm trzecich do analizy zdarzeń.
- **Typ zdarzenia** (kod alfabetyczny). Ten kod jest używany, gdy przeglądasz i przetwarzasz zdarzenia, korzystając z widoków publicznych, dostępnych w bazie danych Kaspersky Security Center, a także podczas eksportowania zdarzeń do systemu SIEM.
- **Opis**. Ten tekst zawiera sytuacje, gdy zdarzenie wystąpi i co należy zrobić w takiej sytuacji.
- **Domyślny czas przechowywania**. To jest liczba dni, przez jaką zdarzenie jest przechowywane w bazie danych Serwera administracyjnego i jest wyświetlane na liście zdarzeń na Serwerze administracyjnym. Po upłynięciu tego czasu, zdarzenie jest usuwane. Jeśli wartość czasu przechowywania zdarzenia to 0, takie zdarzenia są wykrywane, ale nie są wyświetlane na liście zdarzeń na Serwerze administracyjnym. Jeśli skonfigurowałeś zapisywanie takich zdarzeń w dzienniku zdarzeń systemu operacyjnego, znajdziesz je tam.

  Możesz zmienić czas przechowywania zdarzeń:

  - Konsola administracyjna: Ustawianie czasu przechowywania dla zdarzenia
  - Kaspersky Security Center Web Console: Ustawianie czasu przechowywania dla zdarzenia

Inne dane mogą zawierać następujące pola:

- **event_id**: unikatowa liczba zdarzeń w bazie danych, wygenerowana i przypisana automatycznie; nie mylić z **ID typu zdarzenia**.
- **task_id**: identyfikator zadania, które spowodowało wystąpienie zdarzenia (jeśli są jakiekolwiek)
- **severity**: jeden z następujących priorytetów (w kolejności rosnącej):

  0) Niepoprawny priorytet

  1) Informacja

  2) Ostrzeżenie

  3) Błąd

  4) Krytyczny

Zdarzenia Serwera administracyjnego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Serwera administracyjnego.

Zdarzenia krytyczne Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Serwera administracyjnego Kaspersky Security Center, które posiadają priorytet **Krytyczny**.

Zdarzenia krytyczne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domy przech
Limit licencji został przekroczony	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Raz dziennie Kaspersky Security Center sprawdza, czy ograniczenia licencyjne nie są przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją przekracza 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center określa reguły generowania zdarzeń, gdy ograniczenia licencjonowania zostaną przekroczone.	180 dn
Epidemia wirusa	26 (dla	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu	180 dn

	Ochrony plików)		występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	
Epidemia wirusa	27 (dla Ochrony poczty)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dn

Epidemia wirusa	28 (dla Zapory sieciowej)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dn
Zarządzanie urządzeniem nie jest możliwe	4111	KLSRV_HOST_OUT_CONTROL	Zdarzenia tego typu występują, jeśli zarządzane urządzenie jest widoczne w sieci, ale nie ma podłączonego Serwera administracyjnego przez pewien czas. Dowiedz się, co uniemożliwia poprawne działanie Agenta sieciowego na urządzeniu. Możliwe przyczyny obejmują problemy z siecią i usuwanie Agenta sieciowego z urządzenia.	180 dn
Stan urządzenia: Krytyczny	4113	KLSRV_HOST_STATUS_CRITICAL	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Krytyczny*. Możesz skonfigurować warunki, zgodnie z którymi stan	180 dn

			urządzenia zostanie zmieniony na *Krytyczny*.	
Plik klucza został dodany do listy zablokowanych	4124	KLSRV_LICENSE_BLACKLISTED	Zdarzenia tego typu występują, gdy firma Kaspersky dodała kod aktywacyjny lub plik klucza, którego używasz, do listy blokowanych. Aby uzyskać więcej informacji, skontaktuj się z działem pomocy technicznej.	180 dn
Tryb ograniczonej funkcjonalności	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Zdarzenia tego typu występują, gdy Kaspersky Security Center zaczyna działać z podstawową funkcjonalnością, bez funkcji Zarządzanie lukami i poprawkami oraz bez funkcji Zarządzanie urządzeniami mobilnymi. Poniższe elementy są przyczynami i odpowiednimi odpowiedziami na zdarzenie: • Licencja utraciła ważność. Zapewnij licencję do korzystania z trybu pełnej funkcjonalności Kaspersky Security Center (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). • Serwer administracyjny zarządza większą liczbą urządzeń niż określona przez ograniczenie licencji. Przenieś urządzenia z grup administracyjnych Serwera administracyjnego do tych należących	180 dn

			do innego Serwera administracyjnego (jeśli ograniczenie licencji innego Serwera administracyjnego zezwala na to).	
Licencja wkrótce utraci ważność	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Tego typu zdarzenia mają miejsce, gdy zbliża się data wygaśnięcia licencji komercyjnej. Raz dziennie Kaspersky Security Center sprawdza, czy nie zbliża się data wygaśnięcia licencji. Wydarzenia tego typu publikowane są 30 dni, 15 dni, 5 dni i 1 dzień przed datą wygaśnięcia licencji. Nie możesz zmienić liczby dni. Jeśli Serwer administracyjny zostanie wyłączony określonego dnia przed datą wygaśnięcia licencji, zdarzenie nie zostanie opublikowane, aż do następnego dnia. Po wygaśnięciu licencji komercyjnej Kaspersky Security Center zapewnia tylko podstawową funkcjonalność. Możesz zareagować na zdarzenie w następujące sposoby: • Upewnij się, że zapasowy klucz licencyjny został dodany do Serwera administracyjnego. • Jeśli korzystasz z subskrypcji, pamiętaj o jej odnowieniu. Nieograniczona subskrypcja jest odnawiana automatycznie,	180 dn

			jeśli została opłacona w odpowiednim terminie.	
Certyfikat wygasł	4132	KLSRV_CERTIFICATE_EXPIRED	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla Zarządzania urządzeniami mobilnymi utraci ważność. Należy zaktualizować certyfikat, który utracił ważność. Możesz skonfigurować automatyczne aktualizacje certyfikatów, zaznaczając pole **Odnów certyfikat automatycznie, jeśli jest to możliwe** w ustawieniach wydawania certyfikatów.	180 dn
Aktualizacje dla modułów oprogramowania Kaspersky zostały wycofane	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Zdarzenia tego typu występują, jeśli aktualizacje typu seamless zostały wycofane (dla tych aktualizacji wyświetlany jest stan *Wycofano*) przez specjalistów z pomocy technicznej Kaspersky; na przykład, muszą zostać zaktualizowane do nowszej wersji. Zdarzenie dotyczy poprawek Kaspersky Security Center i nie dotyczy modułów zarządzanych aplikacji firmy Kaspersky. Zdarzenie zawiera przyczynę niezainstalowania aktualizacji typu seamless.	180 dn

Zdarzenia błędu funkcyjnego Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Błąd funkcjonalny**.

Zdarzenia błędu funkcyjnego Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyś przecho
Błąd w czasie wykonywania	4125	KLSRV_RUNTIME_ERROR	Zdarzenia tego typu występują w wyniku nieznanych problemów. Najczęściej są to problemy z systemem DBMS, problemy z siecią oraz inne problemy z oprogramowaniem i sprzętem. Szczegóły zdarzenia można znaleźć w opisie zdarzenia.	180 dni
Przekroczono limit instalacji dla jednej z grup licencjonowanych aplikacji	4126	KLSRV_INVLICPROD_EXCEDED	Serwer administracyjny generuje zdarzenia tego typu okresowo (co godzinę). Zdarzenia tego typu występują, jeśli w Kaspersky Security Center zarządzasz kluczami licencyjnymi aplikacji innych firm i jeśli liczba instalacji przekroczyła ograniczenie ustawione przez klucz licencyjny aplikacji innej firmy. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń aplikację innej firmy z urządzeń, na których aplikacja nie jest używana. • Użyj licencji innej firmy dla większej liczby urządzeń.	180 dni

			Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji. Grupa licencjonowanych aplikacji zawiera aplikacje firm trzecich spełniające kryteria ustalone przez Ciebie.	
Przeszukanie segmentu chmury nie powiodło się	4143	KLSRV_KLCLOUD_SCAN_ERROR	Zdarzenia tego typu mają miejsce, gdy serwer administracyjny nie może przeszukać segmentu sieci w środowisku chmury. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio.	Nie jest przecho
Kopiowanie aktualizacji do określonego folderu nie powiodło się	4123	KLSRV_UPD_REPL_FAIL	Zdarzenia tego typu występują, gdy aktualizacje oprogramowania są kopiowane do dodatkowych folderów współdzielonych. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy konto użytkownika, który ma uzyskać dostęp do folderu(ów) posiada prawo do zapisu. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu(ów) uległy zmianie. • Sprawdź połączenie z internetem, gdyż to może być przyczyną zdarzenia. Aby	180 dni

			zaktualizować bazy danych i moduły oprogramowania, postępuj zgodnie z instrukcjami.	
Brak wolnego miejsca na dysku	4107	KLSRV_DISK_FULL	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	180 dni
Folder współdzielony nie jest dostępny	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Zdarzenia tego typu występują, jeśli folder współdzielony Serwera administracyjnego jest niedostępny. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy Serwer administracyjny (na którym znajduje się folder współdzielony) jest włączony i dostępny. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu uległy zmianie. • Sprawdź połączenie sieciowe.	180 dni
Baza danych Serwera administracyjnego jest niedostępna	4109	KLSRV_DATABASE_UNAVAILABLE	Zdarzenia tego typu występują, jeśli baza danych Serwera administracyjnego stała się niedostępna. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy zdalny serwer, na	180 dni

			którym jest zainstalowany serwer SQL, jest dostępny. • Przejrzyj raporty systemu DBMS, aby odkryć przyczynę braku dostępności bazy danych Serwera administracyjnego. Na przykład, ze względu na profilaktyczną obsługę, zdalny serwer z zainstalowanym serwerem SQL może być niedostępny.	
Brak wolnego miejsca w bazie danych Serwera administracyjnego	4110	KLSRV_DATABASE_FULL	Zdarzenia tego typu występują, gdy nie ma wolnego miejsca w bazie danych Serwera administracyjnego. Serwer administracyjny nie działa, gdy jego baza danych osiągnęła swoją pojemność i gdy dalsze zapisywanie w bazie danych nie jest możliwe. Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie: • Korzystasz z SQL Server Express Edition DBMS:	180 dni

			W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego przekroczyła ograniczenie rozmiaru bazy danych. Ograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. W bazie danych Serwera administracyjnego istnieje zbyt dużo zdarzeń wysłanych przez komponent Kontrola aplikacji. Możesz zmienić ustawienia zasady Kaspersky Endpoint Security for Windows dotyczące przechowywania zdarzeń Kontroli aplikacji w bazie danych Serwera administracyjnego. • Używasz systemu DBMS innego niż SQL Server Express Edition: Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Zmniejszanie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.

			Przeglądanie informacji dotyczących wyboru systemu DBMS.	

Zdarzenia ostrzegające Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Ostrzeżenie**.

Zdarzenia ostrzegające Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Do prze
Limit licencji został przekroczony	4098	KLSRV_EV_LICENSE_CHECK_100_110	Raz dziennie Kaspersky Security Center sprawdza, czy ograniczenia licencyjne nie są przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją stanowi od 100% do 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu.	90 d

			• Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center określa reguły generowania zdarzeń, gdy ograniczenia licencjonowania zostaną przekroczone.	
Urządzenie było nieaktywne w sieci od dłuższego czasu	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan Ostrzeżenie. Najczęściej dzieje się tak, gdy zarządzane urządzenie zostaje wycofane z eksploatacji. Możesz zareagować na zdarzenie w następujące sposoby: • W celu usunięcia urządzenia z listy zarządzanych urządzeń: • Określ przedział czasu, po którym tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od dłuższego czasu**, przy użyciu Konsoli administracyjnej lub przy użyciu Kaspersky Security Center Web Console. • Określ przedział czasu, po którym urządzenie zostanie automatycznie usunięte z grupy, przy użyciu Konsoli administracyjnej lub Kaspersky	90 d

			Security Center Web Console.	
Konflikt nazw urządzeń	4102	KLSRV_EVENT_HOSTS_CONFLICT	Zdarzenia tego typu występują, gdy Serwer administracyjny traktuje dwa lub więcej zarządzanych urządzeń jako jedno urządzenie. Ma to miejsce najczęściej wtedy, gdy sklonowany dysk twardy został użyty do wdrożenia oprogramowania na zarządzanych urządzeniach i bez przełączania Agenta sieciowego do trybu klonowania dedykowanego dysku na odpowiednim urządzeniu. Aby uniknąć tego problemu, przełącz Agenta sieciowego do trybu klonowania dysku na odpowiednim urządzeniu przed sklonowaniem dysku twardego tego urządzenia.	90 c
Stan urządzenia: Ostrzeżenie	4114	KLSRV_HOST_STATUS_WARNING	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Ostrzeżenie*. Możesz skonfigurować warunki, zgodnie z którymi stan urządzenia zostanie zmieniony na *Ostrzeżenie*.	90 c
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony	4127	KLSRV_INVLICPROD_FILLED	Zdarzenia tego typu występują, gdy liczba instalacji aplikacji innych firm, zawartych w grupie licencjonowanych aplikacji osiągnie 90% maksymalnej dozwolonej wartości określonej we właściwościach klucza licencyjnego.	90 c

			Możesz zareagować na zdarzenie w następujące sposoby: • Jeśli aplikacja innej firmy nie jest używana na niektórych zarządzanych urządzeniach, usuń aplikację z tych urządzeń. • Jeśli spodziewasz się, że w najbliższej przyszłości liczba instalacji dla aplikacji innej firmy przekroczy dozwoloną maksymalną wartość, uwzględnij uzyskanie licencji innej firmy dla większej liczby urządzeń w przyszłości. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji.	
Certyfikat został zażądany	4133	KLSRV_CERTIFICATE_REQUESTED	Zdarzenia tego typu występują, gdy certyfikat dla Zarządzania urządzeniami mobilnymi nie zostanie automatycznie wystawiony ponownie. Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Automatyczne ponowne wystawienie zostało zainicjowane dla certyfikatu, dla którego wyłączona jest opcja **Odnów certyfikat**	90 c

			automatycznie, jeśli jest to możliwe. Może to być spowodowane błędem, który wystąpił podczas tworzenia certyfikatu. Konieczne może być ręczne ponowne wystawienie certyfikatu. • Jeśli korzystasz z integracji z infrastrukturą klucza publicznego, przyczyną może być brak atrybutu SAM-Account-Name konta użytego do integracji z PKI oraz do wystawienia certyfikatu. Przejrzyj właściwości konta.	
Certyfikat został usunięty	4134	KLSRV_CERTIFICATE_REMOVED	Zdarzenia tego typu występują, gdy administrator usunie dowolny typ certyfikatu (Ogólny, Poczta, VPN) dla Zarządzania urządzeniami mobilnymi. Po usunięciu certyfikatu urządzenia mobilne, podłączone za pośrednictwem tego certyfikatu, nie nawiążą połączenia z Serwerem administracyjnym. To zdarzenie może być pomocne podczas sprawdzania problemów z działaniem, skojarzonych z zarządzaniem urządzeń mobilnych.	90 c
Certyfikat APNs wygasł	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Zdarzenia tego typu występują, gdy	Nie j prze

			certyfikat APNs utraci ważność. Należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM.	
Certyfikat APNs wkrótce utraci ważność	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Zdarzenia tego typu występują, gdy do wygaśnięcia certyfikatu APNs pozostało mniej niż 14 dni. Jeśli certyfikat APNs utraci ważność, należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM. Zalecane jest wcześniejsze utworzenie terminarza odnawiania certyfikatu APNs.	Nie prze
Błąd podczas przesyłania wiadomości FCM do urządzenia mobilnego	4138	KLSRV_GCM_DEVICE_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Google Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android, a FCM Server nie obsłuży żądań otrzymanych z Serwera administracyjnego. To oznacza, że niektóre zarządzane urządzenia mobilne nie otrzymają powiadomienia push.	90 d

			Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z FCM Server i powiązanych błędów można znaleźć w dokumentacji do usługi Google Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie").	
Błąd HTTP podczas wysyłania wiadomości FCM do serwera FCM	4139	KLSRV_GCM_HTTP_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Google Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android, a FCM Server przywróci żądanie Serwera administracyjnego z kodem HTTP innym niż 200 (OK). Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Problemy po stronie serwera FCM. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z FCM Server i powiązanych błędów można znaleźć w dokumentacji do usługi Google	90 c

			Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie”). • Problemy po stronie serwera proxy (jeśli korzystasz z serwera proxy). Przeczytaj kod HTTP w szczegółach zdarzenia i zareaguj odpowiednio.	
Błąd podczas przesyłania wiadomości FCM do serwera FCM	4140	KLSRV_GCM_GENERAL_ERROR	Zdarzenia tego typu występują w wyniku niespodziewanych błędów po stronie Serwera administracyjnego podczas pracy z protokołem Google Firebase Cloud Messaging HTTP. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio. Jeżeli nie znajdziesz rozwiązania swojego problemu, skontaktuj się z działem pomocy technicznej firmy Kaspersky.	90 c
Pozostała niewielka ilość wolnego miejsca na dysku twardym	4105	KLSRV_NO_SPACE_ON_VOLUMES	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, prawie zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	90 c
Mała ilość wolnego miejsca w bazie danych Serwera administracyjnego	4106	KLSRV_NO_SPACE_IN_DATABASE	Zdarzenia tego typu występują, jeśli miejsce w bazie danych Serwera administracyjnego jest zbyt ograniczone. Jeśli nie rozwiążesz tego problemu, wkrótce baza danych Serwera	90 c

				administracyjnego osiągnie swoją pojemność, a Serwer administracyjny nie będzie działał. Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie. Korzystasz z SQL Server Express Edition DBMS: • W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego zaraz osiągnie ograniczenie rozmiaru bazy danych. • Ograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • W bazie danych Serwera administracyjnego istnieje zbyt dużo zdarzeń wysłanych przez komponent Kontrola aplikacji. Możesz zmienić ustawienia zasady Kaspersky Endpoint Security for Windows dotyczące przechowywania zdarzeń Kontroli aplikacji w bazie danych Serwera administracyjnego.

			Używasz systemu DBMS innego niż SQL Server Express Edition: • Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	
Połączenie z podrzędnym Serwerem administracyjnym zostało zerwane	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z podrzędnym Serwerem administracyjnym zostanie przerwane. Przeczytaj dziennik zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany podrzędny Serwer administracyjny i zareaguj odpowiednio.	90 d
Połączenie z głównym Serwerem administracyjnym zostało zerwane	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z głównym Serwerem administracyjnym zostanie przerwane. Przeczytaj dziennik zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany główny Serwer administracyjny i zareaguj odpowiednio.	90 d
Zarejestrowano nowe aktualizacje dla modułów oprogramowania Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Zdarzenia tego typu występują, gdy Serwer administracyjny zarejestruje nowe aktualizacje dla oprogramowania firmy Kaspersky,	90 d

			zainstalowanego na zarządzanych urządzeniach, których instalacja wymaga zatwierdzenia. Zatwierdź lub odrzuć aktualizacje, korzystając z Konsoli administracyjnej lub Kaspersky Security Center Web Console.	
Przekroczono limit wydarzeń w bazie danych. Rozpoczęto usuwanie wydarzeń	4145	KLSRV_EVP_DB_TRUNCATING	Zdarzenia tego typu występują, jeśli usuwanie starszych zdarzeń z bazy danych Serwera administracyjnego rozpoczęło się, gdy pojemność bazy danych Serwera administracyjnego została osiągnięta. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	Nie prze
Przekroczono limit wydarzeń w bazie danych. Usunięto wydarzenia	4146	KLSRV_EVP_DB_TRUNCATED	Zdarzenia tego typu występują, jeśli starsze zdarzenia zostały usunięte z bazy danych Serwera administracyjnego po osiągnięciu pojemności bazy danych Serwera administracyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej dozwolonej liczby	Nie prze

			zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	

Zdarzenia informacyjne Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Informacja**.

Zdarzenia informacyjne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Ponad 90% tego klucza licencyjnego jest wykorzystane	4097	KLSRV_EV_LICENSE_CHECK_90	30 dni
Wykryto nowe urządzenie	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 dni
Urządzenie zostało automatycznie dodane do grupy	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 dni
Urządzenie zostało usunięte z grupy: nieaktywność w sieci od dłuższego czasu	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 dni
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony (wykorzystywanych jest więcej niż 95%)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 dni
Wykryto pliki do przesłania do firmy Kaspersky w celu analizy	4131	KLSRV_APS_FILE_APPEARED	30 dni
ID instancji FCM na tym urządzeniu mobilnym zmieniło się	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 dni
Aktualizacje zostały pomyślnie skopiowane do wskazanego folderu	4122	KLSRV_UPD_REPL_OK	30 dni
Nawiązano połączenie z podrzędnym Serwerem administracyjnym	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 dni

Nawiązano połączenie z głównym Serwerem administracyjnym	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 dni
Bazy danych zostały zaktualizowane	4144	KLSRV_UPD_BASES_UPDATED	30 dni
Audyt: Połączenie z Serwerem administracyjnym zostało nawiązane	4147	KLAUD_EV_SERVERCONNECT	30 dni
Audyt: Obiekt został zmodyfikowany	4148	KLAUD_EV_OBJECTMODIFY	30 dni
Audyt: Stan obiektu zmienił się	4150	KLAUD_EV_TASK_STATE_CHANGED	30 dni
Audyt: Ustawienia grupy zostały zmodyfikowane	4149	KLAUD_EV_ADMGROUP_CHANGED	30 dni
Audyt: Połączenie z Serwerem administracyjnym zostało zakończone	4151	KLAUD_EV_SERVERDISCONNECT	30 dni
Audyt: Właściwości obiektu zostały zmodyfikowane	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 dni
Audyt: uprawnienia użytkownika zostały zmodyfikowane	4153	KLAUD_EV_OBJECTACLMODIFIED	30 dni
Audyt: Klucze szyfrowania zostały zaimportowane lub wyeksportowane z Serwera administracyjnego	5100	KLAUD_EV_DPEKEYSEXPORT	30 dni

Zdarzenia Agenta sieciowego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Agenta sieciowego.

Zdarzenia błędu funkcyjnego Agenta sieciowego

Poniższa tabela wyświetla typy zdarzeń Agenta sieciowego Kaspersky Security Center, których priorytet to **Błąd funkcjonalny**.

Zdarzenia błędu funkcyjnego Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny cz przechowywa
Błąd podczas instalacji aktualizacji	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli automatyczne aktualizowanie i	30 dni

			instalowanie poprawek dla składników Kaspersky Security Center nie zakończyło się pomyślnie. Zdarzenie nie dotyczy aktualizacji zarządzanych aplikacji firmy Kaspersky. Przeczytaj opis zdarzenia. Przyczyną tego zdarzenia może być problem z systemem Windows na Serwerze administracyjnym. Jeśli w opisie wspomniany jest jakikolwiek problem z konfiguracją systemu Windows, rozwiąż ten problem.	
Instalacja aktualizacji oprogramowania firmy trzeciej nie powiodła się	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli używane są funkcje Zarządzanie lukami i poprawkami i Zarządzanie urządzeniami mobilnymi oraz jeśli aktualizacja oprogramowania innych firm nie zakończyła się pomyślnie. Sprawdź, czy odnośnik do oprogramowania innej firmy jest ważny. Przeczytaj opis zdarzenia.	30 dni
Zainstalowanie aktualizacji Windows Update nie powiodło się	7717	KLNAG_EV_WUA_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli aktualizacje systemu Windows nie zakończyły się pomyślnie.	30 dni

			Konfiguruj aktualizacji systemu Windows w profilu Agenta sieciowego. Przeczytaj opis zdarzenia. Poszukaj błędu w Bazie wiedzy Microsoft. Skontaktuj się z pomocą techniczną Microsoft, jeśli sam nie możesz rozwiązać problemu.	

Zdarzenia ostrzegające Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center, które posiadają priorytet **Ostrzeżenie**.

Zdarzenia ostrzegające Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Proces instalacji aktualizacji modułów oprogramowania zwrócił ostrzeżenie	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została zakończona ostrzeżeniem	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została odroczona	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 dni
Wystąpił incydent	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN nie powiodło się	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 dni

Zdarzenia informacyjne Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center, które posiadają priorytet **Informacja**.

Zdarzenia informacyjne Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Aktualizacja modułów aplikacji została pomyślnie zainstalowana	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Instalacja aktualizacji modułów oprogramowania została uruchomiona	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 dni
Aplikacja została zainstalowana	7703	KLNAG_EV_INV_APP_INSTALLED	30 dni
Aplikacja została odinstalowana	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 dni
Monitorowana aplikacja została zainstalowana	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 dni
Monitorowana aplikacja została odinstalowana	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 dni
Aplikacja innego producenta została zainstalowana	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 dni
Dodano nowe urządzenie	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dni
Urządzenie zostało usunięte	7709	KLNAG_EV_DEVICE_REMOVE	30 dni
Wykryto nowe urządzenie	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dni
Urządzenie zostało zautoryzowane	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dni
Udostępnianie pulpitu Windows: Plik został odczytany	7712	KLUSRLOG_EV_FILE_READ	30 dni
Udostępnianie pulpitu Windows: Plik został zmodyfikowany	7713	KLUSRLOG_EV_FILE_MODIFIED	30 dni
Udostępnianie pulpitu Windows: Aplikacja została uruchomiona	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 dni
Udostępnianie pulpitu Windows:	7715	KLUSRLOG_EV_WDS_BEGIN	30 dni

Uruchomiono			
Udostępnianie pulpitu Windows: Zatrzymano	7716	KLUSRLOG_EV_WDS_END	30 dni
Aktualizacja oprogramowania firmy trzeciej została pomyślnie zainstalowana	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została uruchomiona	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN zostało pomyślnie zakończone	7719	KSNPROXY_STARTED_CON_CHK_OK	30 dni
KSN Proxy został zatrzymany	7720	KSNPROXY_STOPPED	30 dni

Zdarzenia serwera iOS MDM

Ta sekcja zawiera informacje o zdarzeniach dotyczących serwera iOS MDM.

Zdarzenia błedu funkcjonalnego serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Błąd funkcjonalny**.

Zdarzenia błedu funkcjonalnego serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Pobranie listy profili nie powiodło się	PROFILELIST_COMMAND_FAILED	30 dni
Instalacja profilu nie powiodła się	INSTALLPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu nie powiodło się	REMOVEPROFILE_COMMAND_FAILED	30 dni
Pobranie listy profili informacyjnych nie powiodło się	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 dni
Instalacja profilu	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 dni

informacyjnego nie powiodła się		
Usunięcie profilu informacyjnego nie powiodło się	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu informacyjnego nie powiodło się	CERTIFICATELIST_COMMAND_FAILED	30 dni
Pobranie listy zainstalowanych aplikacji nie powiodło się	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 dni
Pobranie ogólnych informacji o urządzeniu mobilnym nie powiodło się	DEVICEINFORMATION_COMMAND_FAILED	30 dni
Pobranie informacji o zabezpieczeniach nie powiodło się	SECURITYINFO_COMMAND_FAILED	30 dni
Zablokowanie urządzenia mobilnego nie powiodło się	DEVICELOCK_COMMAND_FAILED	30 dni
Zresetowanie hasła nie powiodło się	CLEARPASSCODE_COMMAND_FAILED	30 dni
Usunięcie danych z urządzenia mobilnego nie powiodło się	ERASEDEVICE_COMMAND_FAILED	30 dni
Instalacja aplikacji nie powiodła się	INSTALLAPPLICATION_COMMAND_FAILED	30 dni
Ustawienie kodu wykupu dla aplikacji nie powiodło się	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 dni
Pobranie listy zarządzanych aplikacji nie powiodło się	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 dni
Usunięcie zarządzanej aplikacji nie powiodło się	REMOVEAPPLICATION_COMMAND_FAILED	30 dni
Ustawienia roamingu zostały odrzucone	SETROAMINGSETTINGS_COMMAND_FAILED	30 dni
Wystąpił błąd działania aplikacji	PRODUCT_FAILURE	30 dni
Wynik polecenia zawiera niepoprawne dane	MALFORMED_COMMAND	30 dni
Przesłanie powiadomienia push nie powiodło się	SEND_PUSH_NOTIFICATION_FAILED	30 dni
Wysłanie polecenia nie powiodło się	SEND_COMMAND_FAILED	30 dni
Nie odnaleziono urządzenia	DEVICE_NOT_FOUND	30 dni

Zdarzenia ostrzegające serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Ostrzeżenie**.

Zdarzenia ostrzegające serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Wykryto próbę podłączenia zablokowanego urządzenia mobilnego	INACTICE_DEVICE_TRY_CONNECTED	30 dni
Profil został usunięty	MDM_PROFILE_WAS_REMOVED	30 dni
Wykryto próbę ponownego użycia certyfikatu klienta	CLIENT_CERT_ALREADY_IN_USE	30 dni
Wykryto nieaktywne urządzenie	FOUND_INACTIVE_DEVICE	30 dni
Wymagany jest kod wykupu	NEED_REDEMPTION_CODE	30 dni
Profil zawarty w zasadach został usunięty z urządzenia	UMDM_PROFILE_WAS_REMOVED	30 dni

Zdarzenia informacyjne serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Informacja**.

Zdarzenia informacyjne serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Podłączono nowe urządzenie mobilne	NEW_DEVICE_CONNECTED	30 dni
Lista profili została pomyślnie pobrana	PROFILELIST_COMMAND_SUCCESSFULL	30 dni
Profil został pomyślnie zainstalowany	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 dni
Profil został pomyślnie usunięty	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 dni
Lista profili informacyjnych została pomyślnie pobrana	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 dni
Profil informacyjny został pomyślnie zainstalowany	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dni
Profil informacyjny został pomyślnie usunięty	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dni

Lista certyfikatów cyfrowych została pomyślnie pobrana	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 dni
Lista zainstalowanych aplikacji została pomyślnie zażądana	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dni
Ogólne informacje o urządzeniu mobilnym zostały pomyślnie pobrane	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 dni
Informacje o zabezpieczeniach zostały pomyślnie pobrane	SECURITYINFO_COMMAND_SUCCESSFULL	30 dni
Urządzenie mobilne zostało pomyślnie zablokowane	DEVICELOCK_COMMAND_SUCCESSFULL	30 dni
Hasło zostało pomyślnie zresetowane	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 dni
Dane zostały pomyślnie usunięte z urządzenia mobilnego	ERASEDEVICE_COMMAND_SUCCESSFULL	30 dni
Aplikacja została pomyślnie zainstalowana	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 dni
Kod wykupu aplikacji został pomyślnie ustawiony dla aplikacji	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 dni
Lista zarządzanych aplikacji została pomyślnie pobrana	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dni
Zarządzana aplikacja została pomyślnie usunięta	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 dni
Ustawienia roamingu zostały pomyślnie zastosowane	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 dni

Zdarzenia serwera urządzeń mobilnych Exchange

Ta sekcja zawiera informacje o zdarzeniach dotyczących serwera urządzeń mobilnych Exchange.

Zdarzenia błędu funkcjonalnego serwera urządzeń mobilnych Exchange

Poniższa tabela wyświetla zdarzenia serwera urządzeń mobilnych Exchange Kaspersky Security Center, które posiadają priorytet **Błąd funkcjonalny**.

Zdarzenia błędu funkcjonalnego serwera urządzeń mobilnych Exchange

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Usunięcie danych z urządzenia mobilnego nie powiodło się	WIPE_FAILED	30 dni
Nie można usunąć informacji o połączeniu urządzeń mobilnych ze skrzynkami pocztowymi	DEVICE_REMOVE_FAILED	30 dni
Zastosowanie profilu ActiveSync w skrzynce pocztowej nie powiodło się	POLICY_APPLY_FAILED	30 dni
Błąd działania aplikacji	PRODUCT_FAILURE	30 dni
Modyfikacja stanu funkcjonalności ActiveSync nie powiodła się	CHANGE_ACTIVE_SYNC_STATE_FAILED	30 dni

Zdarzenia informacyjne serwera urządzeń mobilnych Exchange

Poniższa tabela wyświetla zdarzenia serwera urządzeń mobilnych Exchange Kaspersky Security Center, które posiadają priorytet **Informacja**.

Zdarzenia informacyjne serwera urządzeń mobilnych Exchange

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Podłączono nowe urządzenie mobilne	NEW_DEVICE_CONNECTED	30 dni
Dane zostały pomyślnie usunięte z urządzenia mobilnego	WIPE_SUCCESSFULL	30 dni

Blokowanie często występujących zdarzeń

Ta sekcja zawiera informacje dotyczące zarządzania blokowaniem często występujących zdarzeń, usuwania blokowania często występujących zdarzeń oraz eksportowania listy często występujących zdarzeń do pliku.

Informacje o blokowaniu często występujących zdarzeń

Zarządzana aplikacja, na przykład Kaspersky Endpoint Security for Windows, zainstalowana na jednym lub kilku zarządzanych urządzeniach, może wysyłać wiele zdarzeń tego samego typu do Serwera administracyjnego. Otrzymywanie częstych zdarzeń może przeciążyć bazę danych Serwera administracyjnego i nadpisać inne zdarzenia. Serwer administracyjny zaczyna blokować najczęstsze zdarzenia, gdy liczba wszystkich odebranych zdarzeń przekracza określony limit dla bazy danych.

Serwer administracyjny blokuje automatyczne odbieranie często występujących zdarzeń. Nie możesz samodzielnie blokować często występujących zdarzeń ani wybierać, które zdarzenia mają być blokowane.

Jeśli chcesz dowiedzieć się, czy zdarzenie jest zablokowane, możesz sprawdzić, czy to zdarzenie jest obecne w sekcji **Blokowanie często występujących zdarzeń** właściwości Serwera administracyjnego. Jeśli zdarzenie jest zablokowane, możesz wykonać następujące czynności:

- Jeśli chcesz zapobiec nadpisywaniu bazy danych, możesz kontynuować blokowanie odbieranie tego typu zdarzeń.
- Jeśli chcesz, na przykład, znaleźć przyczynę wysyłania często występujących zdarzeń na Serwer administracyjny, możesz odblokować często występujące zdarzenia i mimo wszystko nadal otrzymywać tego typu zdarzenia.
- Jeśli chcesz nadal otrzymywać często występujące zdarzenia, dopóki nie zostaną ponownie zablokowane, możesz usunąć z blokowania często występujące zdarzenia.

Zarządzanie blokowaniem często występujących zdarzeń

Serwer administracyjny automatycznie blokuje odbieranie często występujących zdarzeń, ale możesz zatrzymać blokowanie i nadal odbierać często występujące zdarzenia. Możesz także zablokować odbieranie często występujących zdarzeń, które wcześniej odblokowałeś.

W celu zarządzania blokowaniem często występujących zdarzeń:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Blokowanie często występujących zdarzeń**.
3. W sekcji **Blokowanie często występujących zdarzeń**:
   - Wybierz opcje **Typ zdarzenia** zdarzeń, których odbieranie chcesz zablokować.
   - Odznacz opcje **Typ zdarzenia** zdarzeń, które chcesz nadal otrzymywać.
4. Kliknij przycisk **Zastosuj**.
5. Kliknij przycisk **OK**.

Serwer administracyjny odbiera często występujące zdarzenia, dla których usunięto zaznaczenie opcji **Typ zdarzenia** i blokuje odbieranie często występujących zdarzeń, dla których wybrałeś opcję **Typ zdarzenia**.

Usuwanie blokowania często występujących zdarzeń

Możesz usunąć blokowanie często występujących zdarzeń i zacząć je otrzymywać, dopóki Serwer administracyjny nie zablokuje ponownie tego typu często występujących zdarzeń.

W celu usunięcia blokowania często występujących zdarzeń:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.

2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Blokowanie często występujących zdarzeń**.

3. W sekcji **Blokowanie często występujących zdarzeń** kliknij wiersz często występującego zdarzenia, dla którego chcesz usunąć blokowanie.

4. Kliknij przycisk **Usuń**.

Często występujące zdarzenie zostanie usunięte z listy często występujących zdarzeń. Serwer administracyjny będzie odbierał zdarzenia tego typu.

Eksportowanie listy często występujących zdarzeń do pliku

W celu wyeksportowania listy często występujących zdarzeń do pliku:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.

2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Blokowanie często występujących zdarzeń**.

3. Kliknij przycisk **Eksportuj do pliku**.

4. W oknie **Zapisz jako**, które zostanie otwarte, określ ścieżkę dostępu do pliku, do którego chcesz zapisać listę.

5. Kliknij przycisk **Zapisz**.

Wszystkie wpisy z listy często występujących zdarzeń są eksportowane do pliku.

Kontrolowanie zmian w stanie maszyn wirtualnych

Serwer administracyjny przechowuje informacje o stanie zarządzanych urządzeń, takie jak rejestr sprzętu i lista zainstalowanych aplikacji, a także ustawienia zarządzanych aplikacji, zadań i profili. Jeśli maszyna wirtualna funkcjonuje jak zarządzane urządzenie, użytkownik może przywrócić jego stan w dowolnym momencie przy pomocy wcześniej utworzonych zrzutów ekranu maszyny wirtualnej. Informacje o stanie maszyny wirtualnej na Serwerze administracyjnym mogą stać się nieaktualne.

Na przykład administrator utworzył zasadę ochrony na Serwerze administracyjnym o godzinie 12:00, który zaczął funkcjonować na maszynie wirtualnej VM_1 o godzinie 12:01. O godzinie 12:30 użytkownik maszyny wirtualnej VM_1 zmienił jej stan, przywracając ją ze zrzutu ekranu zrobionego o godzinie 11:00. Zasada ochrony przestaje działać na maszynie wirtualnej. Jednakże w przestarzałych informacjach przechowywanych na Serwerze administracyjnym można przeczytać, że profil ochrony na maszynie wirtualnej VM_1 wciąż działa.

Program Kaspersky Security Center pomaga monitorować zmiany w stanie maszyn wirtualnych.

Po każdej synchronizacji z urządzeniem, Serwer administracyjny generuje unikatowy numer ID, który jest przechowywany na urządzeniu i na Serwerze administracyjnym. Przed rozpoczęciem kolejnej synchronizacji Serwer administracyjny porównuje wartości tych numerów ID po obu stronach. Jeśli wartości numerów ID nie zgadzają się, Serwer administracyjny rozpoznaje, że maszyna wirtualna została przywrócona ze zrzutu ekranu. Serwer administracyjny resetuje wszystkie ustawienia profili i zadań, które są aktywne dla maszyny wirtualnej, i wysyła na nią aktualne profile oraz listę zadań grupowych.

Monitorowanie stanu ochrony antywirusowej przy użyciu informacji z rejestru systemu

W celu monitorowania stanu ochrony antywirusowej na urządzeniu klienckim przy użyciu informacji zarejestrowanych przez Agenta sieciowego, w zależności od systemu operacyjnego urządzenia:

- Na urządzeniach działających pod kontrolą systemu Windows:

  1. Otwórz rejestr systemu urządzenia klienckiego (na przykład, lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

  2. Przejdź do gałęzi:

     - W systemach 32-bitowych:
       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - W systemach 64-bitowych:
       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     Rejestr systemu wyświetli informacje o stanie ochrony antywirusowej urządzenia klienckiego.

- Na urządzeniach działających pod kontrolą systemu Linux:

  - Informacje są umieszczane w oddzielnych plikach tekstowych, jeden dla każdego typu danych, znajdujących się w następującym miejscu: /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.

- Na urządzeniach działających pod kontrolą systemu macOS:

  - Informacje są umieszczane w oddzielnych plikach tekstowych, jeden dla każdego typu danych, znajdujących się w następującym miejscu: /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

Stan ochrony antywirusowej odpowiada wartościom kluczy opisanym w tabeli znajdującej się poniżej.

Klucze rejestru i ich możliwe wartości

Klucz (typ danych)	Wartość	Opis
`Protection_LastConnected (REG_SZ)`	DD-MM-RRRR GG-MM-SS	Data i godzina (w formacie UTC) ostatniego połączenia z Serwerem administracyjnym
`Protection_AdmServer (REG_SZ)`	IP, nazwa DNS lub nazwa NetBIOS	Nazwa Serwera administracyjnego zarządzającego urządzeniem
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	Numer kompilacji Agenta sieciowego zainstalowanego na urządzeniu
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (patch1; patch2; ...; patchN)	Pełny numer wersji Agenta sieciowego (z poprawkami) zainstalowanego na urządzeniu
`Protection_HostId (REG_SZ)`	ID urządzenia	ID urządzenia
`Protection_DynamicVM (REG_DWORD)`	0 — nie 1 — tak	Agent sieciowy jest instalowany w dynamicznym trybie VDI

`Protection_AvInstalled (REG_DWORD)`	0 — nie 1 — tak	Aplikacja antywirusowa jest zainstalowana na urządzeniu
`Protection_AvRunning (REG_DWORD)`	0 — nie 1 — tak	Ochrona w czasie rzeczywistym jest włączona na urządzeniu
`Protection_HasRtp (REG_DWORD)`	0 — nie 1 — tak	Moduł ochrony w czasie rzeczywistym jest zainstalowany
`Protection_RtpState (REG_DWORD)`	Stan ochrony w czasie rzeczywistym:	
	0	Nieznany
	1	Wyłączony
	2	Wstrzymane
	3	Uruchamiana
	4	Włączona
	5	Włączona z wysokim poziomem ochrony (maksymalna ochrona)
	6	Włączona z niskim poziomem ochrony (maksymalna szybkość)
	7	Włączona z ustawieniami domyślnymi (zalecanymi)
	8	Włączona z ustawieniami niestandardowymi
	9	Błąd działania
`Protection_LastFscan (REG_SZ)`	DD-MM-RRRR GG-MM-SS	Data i godzina (w formacie UTC) ostatniego pełnego skanowania
`Protection_BasesDate (REG_SZ)`	DD-MM-RRRR GG-MM-SS	Data i godzina (w formacie UTC) opublikowania baz danych aplikacji

Przeglądanie i konfigurowanie działań, gdy urządzenia wykazują brak aktywności

Jeśli urządzenia klienckie w grupie są nieaktywne, możesz otrzymać informacje na ten temat. Możesz także automatycznie usuwać takie urządzenia.

W celu przejrzenia lub skonfigurowania działań, gdy urządzenia w grupie wykazują brak aktywności:

1. W drzewie konsoli kliknij prawym klawiszem myszy nazwę żądanej grupy administracyjnej.
2. Z menu kontekstowego wybierz **Właściwości**.

   Spowoduje to otwarcie okna właściwości grupy administracyjnej.
3. W oknie **Właściwości** przejdź do sekcji **Urządzenia**.
4. Jeśli to konieczne, włącz lub wyłącz następujące opcje:

   - Powiadom administratora, jeżeli urządzenie jest nieaktywne dłużej niż (dni)

Jeśli ta opcja jest włączona, administrator otrzyma powiadomienie o nieaktywnych urządzeniach. Możesz określić przedział czasu, po upływie którego tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od bardzo dawna**. Domyślny przedział czasu wynosi 7 dni.

Domyślnie opcja ta jest włączona.

- Usuń urządzenie z grupy, jeżeli było nieaktywne dłużej niż (dni)

  Jeśli ta opcja jest włączona, możesz określić przedział czasu, po upływie którego urządzenie zostanie automatycznie usunięte z grupy. Domyślny przedział czasu wynosi 60 dni.

  Domyślnie opcja ta jest włączona.

- Dziedzicz z grupy nadrzędnej

  Ustawienia z tej sekcji są dziedziczone od grupy nadrzędnej, w której znajduje się urządzenie klienckie. Jeśli ta opcja jest włączona, ustawienia w sekcji **Aktywność urządzenia w sieci** nie mogą być modyfikowane.

  Ta opcja jest dostępna tylko wtedy, gdy grupa administracyjna posiada grupę nadrzędną.

  Domyślnie opcja ta jest włączona.

- Wymuś dziedziczenie w grupach podrzędnych

  Wartości ustawień zostaną rozesłane do grup potomnych, ale we właściwościach grup potomnych te ustawienia są zablokowane.

  Domyślnie opcja ta jest wyłączona.

5. Kliknij **OK**.

Twoje zmiany zostaną zapisane i zastosowane.

Wyłączanie ogłoszeń Kaspersky

W Kaspersky Security Center Web Console sekcja Ogłoszenia firmy Kaspersky (**Monitorowanie i raportowanie → Ogłoszenia firmy Kaspersky**) zawiera informacje dotyczące Twojej wersji Kaspersky Security Center i zarządzanych aplikacji, zainstalowanych na zarządzanych urządzeniach. Jeśli nie chcesz otrzymywać ogłoszeń firmy Kaspersky, możesz wyłączyć tę funkcję.

Ogłoszenia firmy Kaspersky obejmują dwa rodzaje informacji: ogłoszenia związane z bezpieczeństwem oraz ogłoszenia marketingowe. Możesz wyłączyć ogłoszenia każdego typu osobno.

W celu wyłączenia ogłoszeń związanych z bezpieczeństwem:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz wyłączyć ogłoszenia dotyczące bezpieczeństwa.

2. Kliknij go prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.

3. W otwartym oknie właściwości Serwera administracyjnego, w sekcji **Ogłoszenia Kaspersky** wyłącz opcję **Włącz wyświetlanie ogłoszeń Kaspersky w Kaspersky Security Center Web Console**.

4. Kliknij **OK**.

Ogłoszenia firmy Kaspersky są wyłączone.

Ogłoszenia marketingowe są domyślnie wyłączone. Otrzymujesz ogłoszenia marketingowe tylko wtedy, gdy włączyłeś Kaspersky Security Network (KSN). Możesz wyłączyć tego typu ogłoszenia, wyłączając KSN.

Dostosowanie punktów dystrybucji i bram połączenia

Struktura grup administracyjnych w Kaspersky Security Center pełni następujące funkcje:

- Tworzy zakres zasad

  Istnieje alternatywny sposób stosowania odpowiednich ustawień na urządzeniach przy użyciu *profili zasad*. W tym przypadku ustawiasz zakres zasad ze znacznikami, lokalizacjami urządzeń w jednostkach organizacyjnych Active Directory, członkostwem w grupach zabezpieczeń Active Directory.

- Tworzy zakres zadań grupowych

  Istnieje sposób określania zakresu zadań grupowych, który nie jest oparty na hierarchii grup administracyjnych: korzystanie z zadań dla wyboru urządzeń oraz z zadań dla wskazanych urządzeń.

- Nadaje urządzeniom, wirtualnym Serwerom administracyjnym oraz podrzędnym Serwerom administracyjnym prawa dostępu

- Przypisuje punkty dystrybucji

Podczas tworzenia struktury grup administracyjnych należy wziąć pod uwagę topologię sieci organizacji dla optymalnego przydzielenia punktów dystrybucji. Optymalne przydzielenie punktów dystrybucji pozwala na zmniejszenie ruchu w sieci organizacji.

W zależności od schematu organizacyjnego oraz topologii sieci, w strukturze grup administracyjnych można zastosować następujące standardowe konfiguracje:

- Jedno biuro

- Wiele małych, zdalnych biur

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

Standardowa konfiguracja punktów dystrybucji: Jedno biuro

W standardowej konfiguracji „jedno biuro” wszystkie urządzenia znajdują się w obrębie sieci organizacji i są dla siebie widoczne. Sieć organizacji może zawierać kilka oddzielnych części (sieci lub fragmentów sieci) połączonych ze sobą wąskimi kanałami.

Dostępne są następujące metody tworzenia struktury grup administracyjnych:

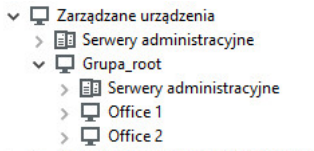
- Tworzenie struktury grup administracyjnych z uwzględnieniem topologii sieci. Struktura grup administracyjnych nie musi odzwierciedlać topologii sieci z absolutną dokładnością. Wystarczy dopasowanie oddzielnych części sieci i pewnych grup administracyjnych. Możesz skorzystać z automatycznego przydzielenia punktów dystrybucji lub zrobić to ręcznie.

- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie punktów dystrybucji, a następnie wskazać jedno lub kilka urządzeń jako punkty dystrybucji dla głównej grupy administracyjnej w każdej z oddzielnych części sieci, na przykład dla grupy **Zarządzane urządzenia**. Wszystkie punkty dystrybucji będą na tym samym poziomie i będą obejmować ten sam obszar, uwzględniając wszystkie urządzenia w sieci organizacji. W takim przypadku każdy z Agentów sieciowych połączy się z punktem dystrybucji o najkrótszej trasie. Trasę do punktu dystrybucji można ustalić za pomocą narzędzia tracert.

Standardowa konfiguracja punktów dystrybucji: Małe zdalne biura

Ta standardowa konfiguracja została utworzona z myślą o małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem internetu. Każde zdalne biuro znajduje się poza NAT, czyli połączenie jednego zdalnego biura z innym jest niemożliwe, gdyż biura są od siebie odizolowane.

Konfiguracja musi być odzwierciedlona w strukturze grup administracyjnych: dla każdego zdalnego biura musi zostać utworzona oddzielna grupa administracyjna (grupy **Office 1** i **Office 2** na rysunku poniżej).



Zdalne biura uwzględnione w strukturze grupy administracyjnej

Do każdej grupy administracyjnej odpowiadającej biuru należy przydzielić jeden lub kilka punktów dystrybucji. Punktami dystrybucji muszą być urządzenia w zdalnym biurze, które posiadają wystarczającą ilość wolnego miejsca na dysku. Urządzenia z grupy **Office 1** będą, na przykład, łączyć się z punktami dystrybucji przydzielonymi do grupy administracyjnej **Office 1**.

Jeśli niektórzy użytkownicy poruszają się między biurami ze swoimi laptopami, w każdym zdalnym biurze, dla grupy administracyjnej najwyższego poziomu (**Główna grupa dla biur** na poniższym rysunku) należy wskazać dwa lub więcej urządzeń jako punkty dystrybucji (oprócz już istniejących punktów dystrybucji).

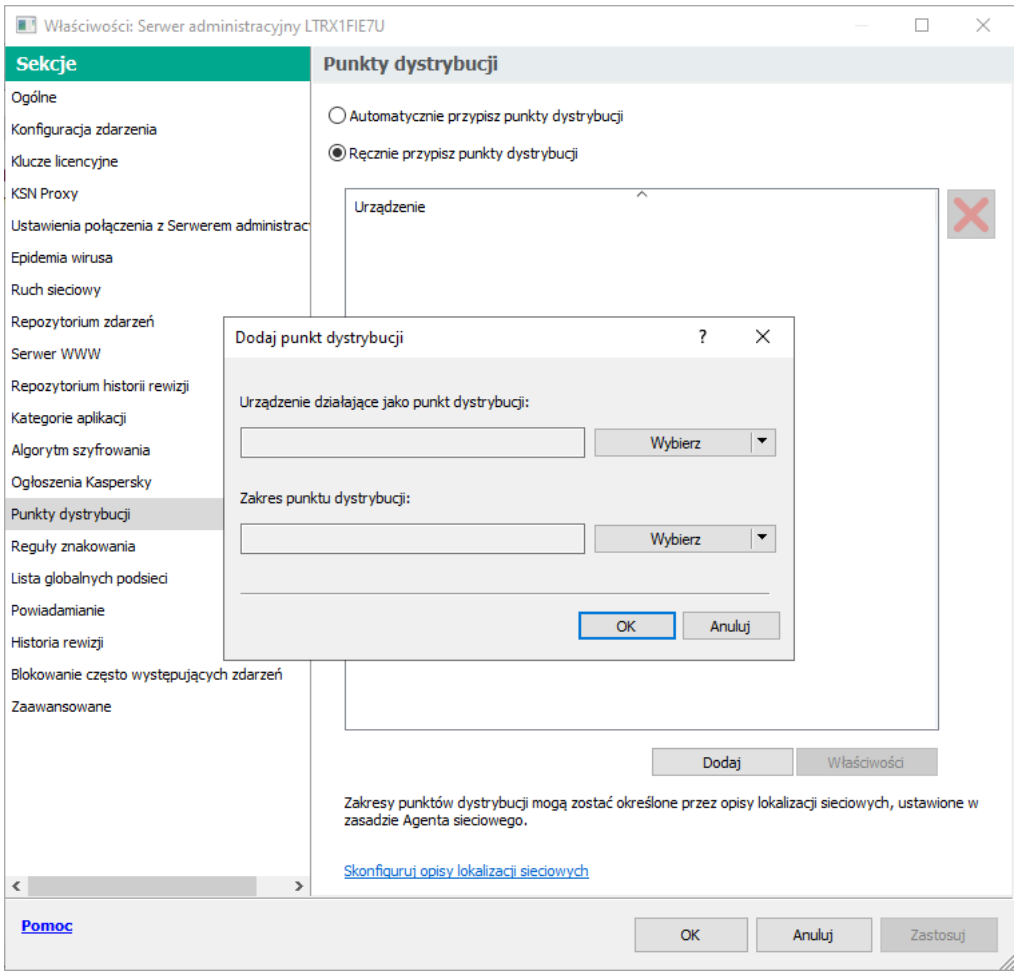
Na przykład: Laptop znajduje się w grupie administracyjnej **Office 1**, a następnie zostaje fizycznie przeniesiony do biura, które odpowiada grupie administracyjnej **Office 2**. Po przeniesieniu laptopa, Agent sieciowy spróbuje połączyć się z punktami dystrybucji przypisanymi do grupy **Office 1**, ale te punkty dystrybucji są niedostępne. Następnie Agent sieciowy próbuje połączyć się z punktami dystrybucji, które zostały przypisane do **Głównej grupy dla biur**. Ponieważ zdalne biura są odizolowane od siebie, próby nawiązania połączenia z punktami dystrybucji przypisanymi do grupy administracyjnej **Główna grupa dla biur** zakończą się pomyślnie tylko wtedy, gdy Agent sieciowy spróbuje połączyć się z punktami dystrybucji w grupie **Office 2**. Oznacza to, że laptop pozostanie w grupie administracyjnej, która odpowiada pierwszemu biuru, ale będzie korzystał z punktu dystrybucji biura, w którym aktualnie się znajduje.

Wskazywanie zarządzanego urządzenia jako punktu dystrybucji

Możesz ręcznie wskazać urządzenie jako punkt dystrybucji dla grupy administracyjnej i skonfigurować go jako bramę połączenia w Konsoli administracyjnej.

W celu wskazania urządzenia jako punktu dystrybucji dla grupy administracyjnej:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
4. W prawej części okna wybierz opcję **Ręcznie przypisz punkty dystrybucji**.
5. Kliknij przycisk **Dodaj**.



Przypisywanie punktów dystrybucji

Zostanie otwarte okno **Dodaj punkt dystrybucji**.

6. W oknie **Dodaj punkt dystrybucji** wykonaj następujące działania:

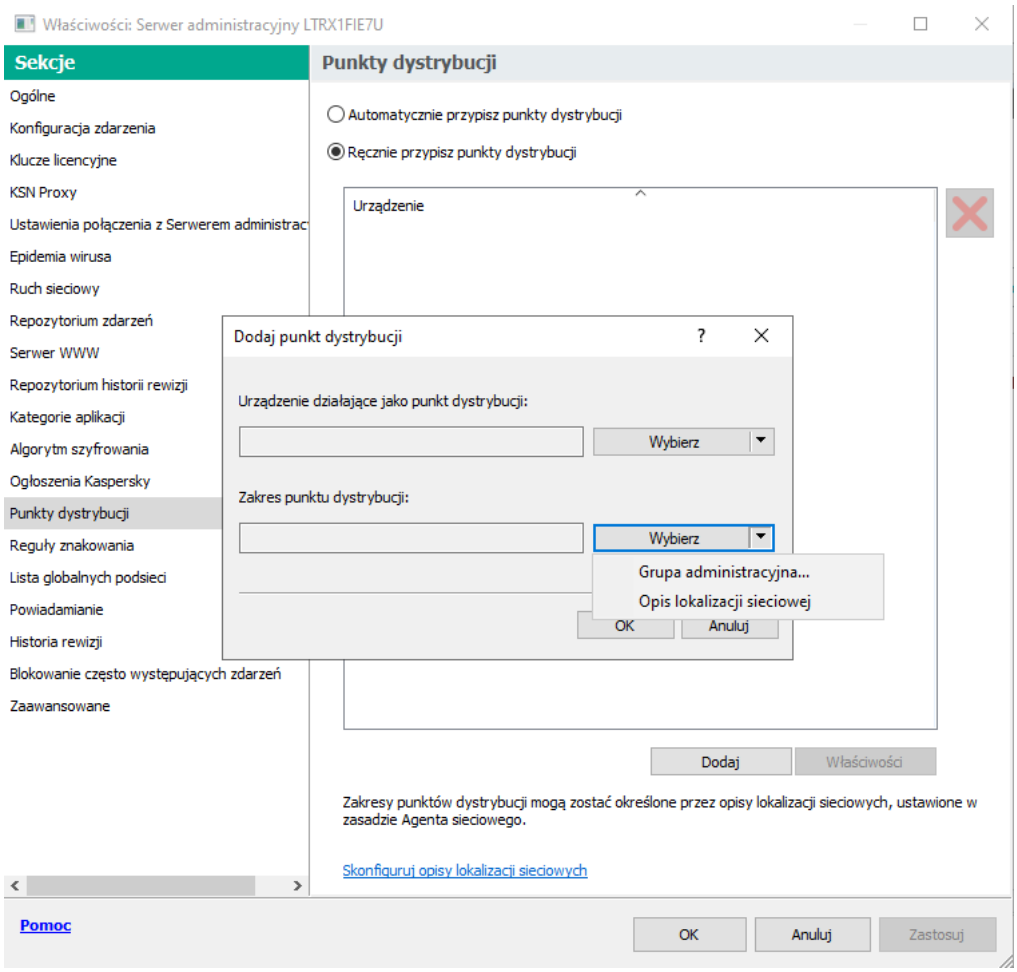
   a. Pod sekcją **Urządzenie**, które ma działać jako punkt dystrybucji kliknij strzałkę (▾) skierowaną w dół obok przycisku **Wybierz** i wybierz opcję **Dodaj urządzenie z grupy**.

   b. W otwartym oknie **Wybierz urządzenia** wybierz urządzenie, które będzie pełniło rolę punktu dystrybucji.

   c. Pod sekcją **Obszar punktu dystrybucji** kliknij strzałkę skierowaną w dół (▾) obok przycisku **Wybierz**.

   d. Wskaż określone urządzenia, na które punkt dystrybucji roześle uaktualnienia. Możesz określić opis grupy administracyjnej lub lokalizacji sieciowej.

   e. Kliknij **OK**, aby zamknąć okno **Dodaj punkt dystrybucji**.



Wybieranie zakresu punktu dystrybucji

Dodany punkt dystrybucji będzie wyświetlany na liście punktów dystrybucji, w sekcji **Punkty dystrybucji**.

Pierwsze urządzenie z zainstalowanym Agentem sieciowym, które nawiąże połączenie z wirtualnym Serwerem administracyjnym, zostanie automatycznie wskazane jako punkt dystrybucji i skonfigurowane jako brama połączenia.

Podłączanie nowego segmentu sieci za pomocą urządzeń Linux

Możesz podłączyć nowy segment sieci do urządzenia z systemem Linux. Potrzebujesz co najmniej dwóch różnych urządzeń. Jedno urządzenie, które można skonfigurować jako bramę połączenia w strefie DMZ; a drugie urządzenie można skonfigurować jako punkt dystrybucji.

Postępuj zgodnie z procedurą w tej sekcji dopiero po zakończeniu głównego scenariusza wdrażania.

W celu podłączenia nowego segmentu sieci na urządzeniu z systemem Linux:

1. Podłącz urządzenie Linux jako bramę połączenia w strefie DMZ.
2. Podłącz urządzenie Linux do Serwera administracyjnego za pośrednictwem bramy połączenia.

Podłączanie nowego segmentu sieci na urządzeniu z systemem Linux zostało skonfigurowane.

Podłączanie urządzenia Linux jako bramy połączenia w strefie zdemilitaryzowanej

W celu podłączenia urządzenia Linux jako bramy połączenia w strefie zdemilitaryzowanej (DMZ):

1. Pobierz i zainstaluj Agenta sieciowego na urządzeniu Linux.
2. Uruchom skrypt poinstalacyjny i postępuj zgodnie z instrukcjami kreatora, aby ustawić konfigurację środowiska lokalnego. W wierszu polecenia uruchom następujące polecenie:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```
3. Na kroku z pytaniem o tryb Agenta sieciowego wybierz opcję **Użyj jako bramy połączenia**.
4. W otwartym oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
5. W otwartym oknie **Punktów dystrybucji**, w prawej części okna:
   a. Wybierz opcję **Ręcznie przypisz punkty dystrybucji**.
   b. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj punkt dystrybucji**.
6. W oknie **Dodaj punkt dystrybucji** wykonaj następujące działania:
   a. W obszarze **Urządzenie**, które ma działać jako punkt dystrybucji, kliknij strzałkę w dół (▾) na przycisku podzielonym **Wybierz**, a następnie wybierz opcję **Dodaj bramę połączenia w DMZ na podstawie adresu**.
   b. Pod sekcją **Obszar punktu dystrybucji** kliknij strzałkę skierowaną w dół (▾) obok przycisku **Wybierz**.
   c. Wskaż określone urządzenia, na które punkt dystrybucji roześle uaktualnienia. Możesz określić grupę administracyjną.
   d. Kliknij **OK**, aby zamknąć okno **Dodaj punkt dystrybucji**.
7. Dodany punkt dystrybucji będzie wyświetlany na liście punktów dystrybucji, w sekcji **Punkty dystrybucji**.
8. Uruchom narzędzie klnagchk, aby sprawdzić, czy połączenie z Kaspersky Security Center zostało pomyślnie skonfigurowane. W wierszu polecenia uruchom:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
9. W menu głównym przejdź do Kaspersky Security Center i wykryj urządzenie.
10. W otwartym oknie kliknij przycisk <Nazwa urządzenia>.
11. Z listy rozwijalnej wybierz odnośnik **Przenieś do grupy**.
12. W otwartym oknie **Wybierz grupy** kliknij odnośnik **Punktów dystrybucji**.
13. Kliknij **OK**.
14. Uruchom ponownie usługę Agenta sieciowego na kliencie Linux, wykonując następujące polecenie w wierszu poleceń:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
```

Podłączanie urządzenia Linux jako bramy połączenia w strefie zdemilitaryzowanej zostało zakończone.

Podłączanie urządzenia Linux do Serwera administracyjnego za pośrednictwem bramy połączenia

Aby podłączyć urządzenie Linux do Serwera administracyjnego za pośrednictwem bramy połączenia, wykonaj następujące czynności na tym urządzeniu:

1. Pobierz i zainstaluj Agenta sieciowego na urządzeniu Linux.
2. Uruchom skrypt poinstalacyjny Agenta sieciowego, wykonując następujące polecenie w wierszu poleceń:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```
3. W kroku z pytaniem o tryb Agenta sieciowego wybierz opcję **Połącz z Serwerem, korzystając z bramy połączenia** i wprowadź adres bramy połączenia.
4. Sprawdź połączenie z Kaspersky Security Center i bramę połączenia, używając następującego polecenia w wierszu polecenia:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   Adres bramy połączenia jest wyświetlany w danych wyjściowych.

Podłączanie urządzenia Linux do Serwera administracyjnego za pośrednictwem bramy połączenia zostało zakończone. Tego urządzenia można używać do dystrybucji aktualizacji, do zdalnej instalacji aplikacji oraz do pobierania informacji o urządzeniach sieciowych.

Dodawanie bramy połączenia w strefie DMZ jako punktu dystrybucji

Brama połączenia oczekuje na połączenia z Serwerem administracyjnym bardziej niż nawiązuje te połączenia z Serwerem administracyjnym. To oznacza, że od razu po zainstalowaniu bramy połączenia na urządzeniu w DMZ, Serwer administracyjny nie wyświetla urządzenia wśród zarządzanych urządzeń. Dlatego też należy przeprowadzić specjalną procedurę w celu zapewnienia, że Serwer administracyjny zainicjuje połączenie z bramą połączenia.

W celu dodania urządzenia z bramą połączenia jako punktu dystrybucji:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
4. W prawej części okna wybierz opcję **Ręcznie przypisz punkty dystrybucji**.
5. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj punkt dystrybucji**.
6. W oknie **Dodaj punkt dystrybucji** wykonaj następujące działania:
   a. W obszarze **Urządzenie, które ma działać jako punkt dystrybucji** kliknij strzałkę w dół (▾) na przycisku podzielonym **Wybierz**, a następnie wybierz opcję **Dodaj bramę połączenia w DMZ na podstawie adresu**.

b. W otwartym oknie **Wprowadź adres bramy połączenia** wprowadź adres IP bramy połączenia (lub wprowadź nazwę, jeśli brama połączenia jest dostępna według nazwy).

c. Pod sekcją **Obszar punktu dystrybucji** kliknij strzałkę skierowaną w dół (▾) obok przycisku **Wybierz**.

d. Wskaż określone urządzenia, na które punkt dystrybucji roześle uaktualnienia. Możesz określić opis grupy administracyjnej lub lokalizacji sieciowej.

Zalecamy posiadanie oddzielnej grupy dla zewnętrznych zarządzanych urządzeń.

Po wykonaniu tych działań, lista punktów dystrybucji zawiera nowy wpis o nazwie **Tymczasowy wpis dla bramy połączenia**.

Serwer administracyjny prawie natychmiast próbuje nawiązać połączenie z bramą połączenia pod podanym adresem. Jeśli się powiedzie, nazwa wpisu zmieni się na nazwę urządzenia bramy połączenia. Ten proces trwa do pięciu minut.

Podczas gdy tymczasowy wpis dla bramy połączenia jest konwertowany na nazwany wpis, brama połączenia pojawia się również w grupie **Nieprzypisane urządzenia**.

Automatyczne przypisywanie punktów dystrybucji

Zalecane jest automatyczne przypisywanie punktów dystrybucji. Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji.

Aby automatycznie przypisać punkty dystrybucji:

1. Otwórz okno główne aplikacji.
2. W drzewie konsoli należy wybrać węzeł z nazwą Serwera administracyjnego, dla którego chcesz automatycznie przypisać punkty dystrybucji.
3. W menu kontekstowym Serwera administracyjnego kliknij **Właściwości**.
4. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Punkty dystrybucji**.
5. W prawej części okna wybierz opcję **Automatycznie przypisz punkty dystrybucji**.

   Jeśli włączone jest automatyczne wskazywanie urządzeń jako punktów dystrybucji, nie można ręcznie skonfigurować punktów dystrybucji, ani też zmodyfikować listy punktów dystrybucji.

6. Kliknij **OK**.

Serwer administracyjny automatycznie przypisze i skonfiguruje punkty dystrybucji.

Informacje o lokalnej instalacji Agenta sieciowego na urządzeniu określonym jako punkt dystrybucji

Aby umożliwić urządzeniu wybranemu na punkt dystrybucji bezpośrednią komunikację z wirtualnym Serwerem administracyjnym tak, aby służył jako brama połączenia, Agent sieciowy musi zostać zainstalowany lokalnie na tym urządzeniu.

Procedura lokalnej instalacji Agenta sieciowego na urządzeniu określonym jako punkt dystrybucji jest identyczna jak lokalna instalacja Agenta sieciowego na dowolnym urządzeniu w sieci.

Dla urządzenia wybranego jako punkt dystrybucji muszą zostać spełnione następujące warunki:

- Podczas lokalnej instalacji Agenta sieciowego określ adres wirtualnego Serwera administracyjnego zarządzającego urządzeniem w polu **Adres serwera**, w oknie **Serwer administracyjny** kreatora instalacji. Można użyć adresu IP lub nazwy urządzenia w sieci Windows.

  Dla adresu Serwera wirtualnego używany jest następujący format: <Pełny adres fizycznego Serwera administracyjnego, do którego należy wirtualny Serwer>/<Nazwa wirtualnego Serwera administracyjnego>.

- Aby mógł on pełnić rolę bramy połączenia, otwórz wszystkie porty urządzenia, które są niezbędne dla komunikacji z Serwerem administracyjnym.

Po zainstalowaniu na tym urządzeniu Agenta sieciowego z określonymi ustawieniami, Kaspersky Security Center automatycznie wykonuje następujące akcje:

- Dodaje to urządzenie do grupy **Zarządzane urządzenia** wirtualnego Serwera administracyjnego.

- Wskazuje to urządzenie jako punkt dystrybucji dla grupy **Zarządzane urządzenia** wirtualnego Serwera administracyjnego.

Konieczne i wystarczające jest przeprowadzenie lokalnej instalacji Agenta sieciowego na urządzeniu wskazanym jako punkt dystrybucji dla grupy **Zarządzane urządzenia** w sieci organizacji. Możesz zainstalować Agenta sieciowego zdalnie na urządzeniach służących jako punkty dystrybucji w zagnieżdżonych grupach administracyjnych. W tym celu użyj punkt dystrybucji grupy **Zarządzane urządzenia** jako bramy połączenia.

Informacje o używaniu punktu dystrybucji jako bramy połączenia

Jeśli Serwer administracyjny znajduje się poza strefą zdemilitaryzowaną (demilitarized zone, DMZ), Agenty sieciowe z tej strefy nie mogą nawiązać połączenia z Serwerem administracyjnym.

Podczas łączenia Serwera administracyjnego z Agentami sieciowymi możesz użyć punktu dystrybucji jako bramy połączenia. Punkt dystrybucji otworzy port dla Serwera administracyjnego w celu nawiązania połączenia. Po uruchomieniu Serwera administracyjnego połączy się on z punktem dystrybucji i utrzyma to połączenie podczas całej sesji.

Po otrzymaniu sygnału z Serwera administracyjnego, punkt dystrybucji wyśle sygnał UDP do Agentów sieciowych w celu zezwolenia na połączenie z Serwerem administracyjnym. Po odebraniu sygnału przez Agenty sieciowe, połączą się one z punktem dystrybucji, który będzie wymieniał informacje między Agentami sieciowymi a Serwerem administracyjnym. Wymiana informacji może odbywać się za pośrednictwem sieci IPv4 lub IPv6.

Zalecane jest użycie jako bramy połączenia specjalnie przypisanego urządzenia oraz przydzielenie do bramy połączenia maksymalnie 10 000 urządzeń klienckich (w tym urządzeń mobilnych).

Dodawanie zakresów IP do listy skanowanych zakresów punktu dystrybucji

Możesz dodać zakresy IP do listy skanowanych zakresów punktu dystrybucji.

W celu dodani zakresu IP do listy skanowanych zakresów:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z otwartego menu kontekstowego węzła wybierz **Właściwości**.
3. W otwartym oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
4. Na liście wybierz żądany punkt dystrybucji i kliknij **Właściwości**.
5. W otwartym oknie właściwości punktów dystrybucji, w lewym panelu **Sekcje** wybierz **Wykrywanie urządzeń** → **Zakresy IP**.
6. Zaznacz pole **Włącz przeszukiwanie zakresów**.
7. Kliknij przycisk **Dodaj**.

   Przycisk **Dodaj** jest aktywny tylko wtedy, gdy zaznaczysz pole **Włącz przeszukiwanie zakresów**.

   Zostanie otwarte okno **Zakres IP**.
8. W oknie **Zakres IP** wprowadź nazwę nowego zakresu IP (domyślna nazwa to Nowy zakres).
9. Kliknij przycisk **Dodaj**.
10. Wykonaj jedną z poniższych czynności:
    - Określ zakres IP, używając początkowego i końcowego adresu IP.
    - Określ zakres IP, używając adresu oraz maski podsieci.
    - Kliknij **Przeglądaj** i dodaj podsieć z globalnej listy podsieci.
11. Kliknij **OK**.
12. Kliknij **OK**, aby dodać nowy zakres z określoną nazwą.

Nowy zakres pojawi się na liście skanowanych zakresów.

Używanie punktu dystrybucji jako serwera push

W Kaspersky Security Center punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego oraz zarządzanych za pośrednictwem agenta sieciowego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

Serwer push obsługuje do 50 000 jednoczesnych połączeń.

Punktów dystrybucji można używać jako serwerów push, aby zapewnić ciągłą łączność między zarządzanym urządzeniem a Serwerem administracyjnym. W przypadku niektórych operacji, takich jak uruchamianie i zatrzymywanie zadań lokalnych, odbieranie statystyk dla zarządzanej aplikacji lub tworzenie tunelu, wymagana jest ciągła łączność. Jeśli używasz punktu dystrybucji jako serwera push, nie musisz używać opcji **Nie odłączaj od Serwera administracyjnego** na zarządzanych urządzeniach lub wysyłaj pakiety do portu UDP Agenta sieciowego.

W celu użycia punktu dystrybucji jako serwera push:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z otwartego menu kontekstowego węzła wybierz **Właściwości**.
3. W otwartym oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
4. Na liście wybierz żądany punkt dystrybucji, a następnie kliknij **Właściwości**.
5. W otwartym oknie właściwości punktu dystrybucji, w sekcji **Ogólne** lewego panelu **Sekcje** wybierz opcję **Użyj tego punktu dystrybucji jako serwera push**.
6. Określ numer portu serwera push, czyli portu na punkcie dystrybucji, którego urządzenia klienckie będą używać do nawiązywania połączeń.

   Domyślnie wykorzystywany jest port 13295.
7. Kliknij przycisk **OK**, aby zamknąć okno właściwości punktu dystrybucji.
8. Otwórz okno właściwości zasady Agenta sieciowego.
9. W sekcji **Łączność** przejdź do podsekcji **Sieć**.
10. W podsekcji **Sieć** wybierz opcję **Użyj punktu dystrybucji do wymuszenia nawiązania połączenia z Serwerem administracyjnym**.
11. Kliknij przycisk **OK**, aby zamknąć okno.

Punkt dystrybucji zacznie działać jako serwer push. Teraz może wysyłać powiadomienia push na urządzenia klienckie.

Jeśli zarządzasz urządzeniami z zainstalowanym KasperskyOS lub planujesz to zrobić, musisz użyć punktu dystrybucji jako serwera push. Możesz także użyć punktu dystrybucji jako serwera push, jeśli chcesz wysłać powiadomienia push na urządzenia klienckie.

Inne podstawowe prace

Ta sekcja zawiera zalecenia dotyczące codziennej pracy z Kaspersky Security Center.

Zarządzanie Serwerami administracyjnymi

Ta sekcja zawiera informacje na temat pracy z Serwerami administracyjnymi i ich konfiguracji.

Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego

Możesz dodać Serwer administracyjny jako podrzędny Serwer administracyjny, a tym samym utworzyć hierarchię „główny/podrzędny". Dodanie podrzędnego Serwera administracyjnego jest możliwe niezależnie od tego, czy Serwer administracyjny, którego zamierzasz używać jako podrzędny, jest dostępny do podłączenia poprzez Konsolę administracyjną.

Podczas łączenia dwóch Serwerów administracyjnych w hierarchię upewnij się, że port 13291 jest dostępny na obu Serwerach administracyjnych. Port 13291 jest wymagany do odbierania połączeń od Konsoli administracyjnej do Serwera administracyjnego.

Podłączanie Serwera administracyjnego jako podrzędnego w odniesieniu do głównego Serwera administracyjnego

Możesz dodać Serwer administracyjny jako podrzędny, podłączając go do głównego Serwera administracyjnego poprzez port 13000. Potrzebne jest urządzenie z zainstalowaną Konsolą administracyjną, z której można uzyskać dostęp do portów TCP o numerze 13291 na obu Serwerach administracyjnych: domniemany główny Serwer administracyjny i domniemany podrzędny Serwer administracyjny.

W celu dodania podrzędnego Serwera administracyjnego, który jest dostępny dla połączenia poprzez Konsolę administracyjną:

1. Upewnij się, że port 13000 przyszłego głównego Serwera administracyjnego jest dostępny do odbierania połączeń od podrzędnych Serwerów administracyjnych.
2. Użyj Konsoli administracyjnej do nawiązywania połączenia z domniemanym głównym Serwerem administracyjnym.
3. Wybierz grupę administracyjną, do której chcesz dodać podrzędny Serwer administracyjny.
4. W obszarze roboczym węzła **Serwery administracyjne** wybranej grupy kliknij odnośnik **Dodaj podrzędny Serwer administracyjny**.

   Zostanie uruchomiony Kreator dodawania podrzędnego Serwera administracyjnego.
5. W pierwszym kroku kreatora (wprowadzanie adresu Serwera administracyjnego dodawanego do grupy) wprowadź nazwę sieci domniemanego podrzędnego Serwera administracyjnego.
6. Postępuj zgodnie z instrukcjami kreatora.

Zostanie utworzona hierarchia „główny/podrzędny". Główny Serwer administracyjny będzie odbierał połączenie od podrzędnego Serwera administracyjnego.

Jeśli nie posiadasz urządzenia z zainstalowaną Konsolą administracyjną, z której można uzyskać dostęp do portów TCP o numerze 13291 na obu Serwerach administracyjnych (jeśli, na przykład, domniemany podrzędny Serwer administracyjny znajduje się w zdalnym biurze, a administrator systemu z tego biura nie może otworzyć dostępu do Internetu dla portu 13291 ze względów bezpieczeństwa), nadal będziesz mógł dodać podrzędny Serwer administracyjny.

W celu dodania podrzędnego Serwera administracyjnego, który nie jest dostępny dla połączenia poprzez Konsolę administracyjną:

1. Upewnij się, że port 13000 domniemanego głównego Serwera administracyjnego jest dostępny dla połączenia z podrzędnych Serwerów administracyjnych.

2. Zapisz plik certyfikatu domniemanego głównego Serwera administracyjnego na urządzeniu zewnętrznym, takim jak dysk flash, lub wyślij go do administratora systemu w zdalnym biurze, w którym znajduje się Serwer administracyjny.

   Plik certyfikatu Serwera administracyjnego znajduje się na tym samym Serwerze administracyjnym, w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Zapisz plik certyfikatu domniemanego podrzędnego Serwera administracyjnego na urządzeniu zewnętrznym, takim jak dysk flash. Jeśli domniemany podrzędny Serwer administracyjny znajduje się w zdalnym biurze, skontaktuj się z administratorem systemu z tego biura, aby poprosić go/ją o przesłanie certyfikatu.

   Plik certyfikatu Serwera administracyjnego znajduje się na tym samym Serwerze administracyjnym, w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. Użyj Konsoli administracyjnej do nawiązywania połączenia z domniemanym głównym Serwerem administracyjnym.

5. Wybierz grupę administracyjną, do której chcesz dodać podrzędny Serwer administracyjny.

6. W obszarze roboczym węzła **Serwery administracyjne** kliknij odnośnik **Dodaj podrzędny Serwer administracyjny**.

   Zostanie uruchomiony Kreator dodawania podrzędnego Serwera administracyjnego.

7. W pierwszym kroku kreatora (wprowadzanie adresu) pozostaw pole **Adres podrzędnego Serwera administracyjnego (opcjonalnie)** puste.

8. W oknie **Plik certyfikatu podrzędnego Serwera administracyjnego** kliknij przycisk **Przeglądaj** i wybierz plik certyfikatu podrzędnego Serwera administracyjnego, który zapisałeś.

9. Po zakończeniu pracy kreatora użyj innej instancji Konsoli administracyjnej do nawiązania połączenia z domniemanym podrzędnym Serwerem administracyjnym. Jeśli ten Serwer administracyjny znajduje się w zdalnym biurze, skontaktuj się z administratorem systemu z tego biura, aby poprosić go/ją o połączenie z domniemanym podrzędnym Serwerem administracyjnym i wykonaj dalsze kroki.

10. Z menu kontekstowego węzła **Serwer administracyjny** wybierz **Właściwości**.

11. We właściwościach Serwera administracyjnego przejdź do sekcji **Zaawansowane**, a następnie do podsekcji **Hierarchia Serwerów administracyjnych**.

12. Zaznacz pole **Ten Serwer administracyjny jest podrzędnym w hierarchii**.

    Pola wejściowe stają się dostępne do wprowadzenia i edycji danych.

13. W polu **Adres głównego Serwera administracyjnego** wprowadź nazwę sieci domniemanego głównego Serwera administracyjnego.

14. Wybierz wcześniej zapisany plik z certyfikatem domniemanego głównego Serwera administracyjnego, klikając przycisk **Przeglądaj**.

15. Kliknij **OK**.

Zostanie utworzona hierarchia „główny/podrzędny". Możesz nawiązać połączenie z podrzędnym Serwerem administracyjnym poprzez Konsolę administracyjną. Główny Serwer administracyjny będzie odbierał połączenie od podrzędnego Serwera administracyjnego.

Nawiązywanie połączenia między głównym Serwerem administracyjnym a podrzędnym Serwerem administracyjnym

Możesz dodać nowy Serwer administracyjny jako podrzędny, aby główny Serwer administracyjny nawiązywał połączenie z podrzędnym Serwerem administracyjnym poprzez port 13000. Jest to zalecane w sytuacjach, gdy, na przykład, umieszczasz podrzędny Serwer administracyjny w strefie DMZ.

Potrzebne jest urządzenie z zainstalowaną Konsolą administracyjną, z której można uzyskać dostęp do portów TCP o numerze 13291 na obu Serwerach administracyjnych: domniemany główny Serwer administracyjny i domniemany podrzędny Serwer administracyjny.

W celu dodania nowego Serwera administracyjnego jako podrzędnego i podłączenia go do głównego Serwera administracyjnego poprzez port 13000:

1. Upewnij się, że port 13000 domniemanego podrzędnego Serwera administracyjnego jest dostępny do odbierania połączeń z głównego Serwera administracyjnego.
2. Użyj Konsoli administracyjnej do nawiązywania połączenia z domniemanym głównym Serwerem administracyjnym.
3. Wybierz grupę administracyjną, do której chcesz dodać podrzędny Serwer administracyjny.
4. W obszarze roboczym węzła **Serwery administracyjne** odpowiedniej grupy administracyjnej kliknij odnośnik **Dodaj podrzędny Serwer administracyjny**.

   Zostanie uruchomiony Kreator dodawania podrzędnego Serwera administracyjnego.
5. W pierwszym kroku kreatora (wprowadzanie adresu Serwera administracyjnego dodawanego do grupy) wprowadź nazwę sieci domniemanego podrzędnego Serwera administracyjnego i zaznacz pole **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**.
6. Jeśli nawiązujesz połączenie z domniemanym podrzędnym Serwerem administracyjnym przy użyciu serwera proxy, w pierwszym kroku kreatora zaznacz pole **Użyj serwera proxy** i określ ustawienia połączenia.
7. Postępuj zgodnie z instrukcjami kreatora.

Hierarchia Serwerów administracyjnych zostanie utworzona. Podrzędny Serwer administracyjny będzie odbierał połączenie od głównego Serwera administracyjnego.

Nawiązywanie połączenia z Serwerem administracyjnym i przełączanie pomiędzy Serwerami administracyjnymi

Po uruchomieniu programu Kaspersky Security Center próbuje on nawiązać połączenie z Serwerem administracyjnym. Jeżeli w sieci jest dostępnych kilka Serwerów administracyjnych, aplikacja będzie próbowała nawiązać połączenie z tym Serwerem, z którym była połączona podczas poprzedniej sesji Kaspersky Security Center.

Jeżeli aplikacja jest uruchamiana po raz pierwszy po jej zainstalowaniu, próbuje nawiązać połączenie z Serwerem administracyjnym określonym podczas instalacji Kaspersky Security Center.

Po nawiązaniu połączenia z Serwerem administracyjnym, drzewo folderów tego Serwera jest wyświetlane w drzewie konsoli.

Jeśli do drzewa konsoli było dodanych kilka Serwerów administracyjnych, możesz się pomiędzy nimi przełączać.

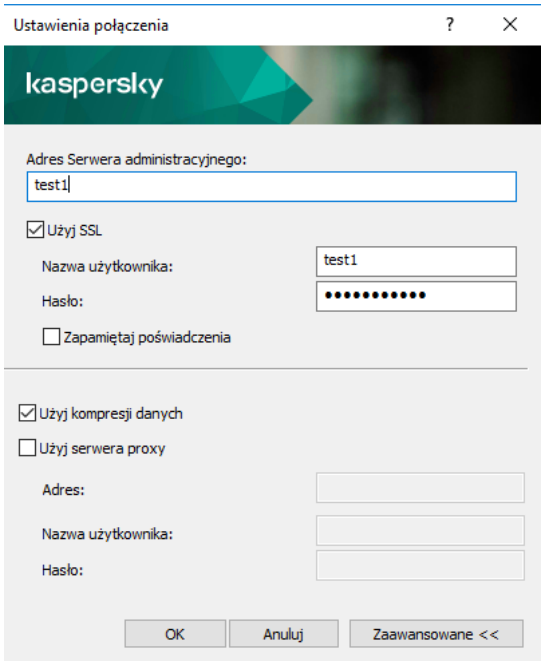
Konsola administracyjna jest wymagana do pracy z każdym Serwerem administracyjnym. Przed pierwszym połączeniem z nowym Serwerem administracyjnym upewnij się, że port 13291, który odbiera połączenia od Konsoli administracyjnej, jest otwarty, a także wszystkie pozostałe porty wymagane do komunikacji między Serwerem administracyjnym a innymi komponentami Kaspersky Security Center.

W celu przełączenia się na inny Serwer administracyjny:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. Z menu kontekstowego węzła wybierz **Połącz z Serwerem administracyjnym**.
3. W otwartym oknie **Ustawienia połączenia**, w polu **Adres Serwera administracyjnego** określ nazwę Serwera administracyjnego, z którym chcesz nawiązać połączenie. Jako nazwę Serwera administracyjnego można określić adres IP lub nazwę urządzenia w sieci Windows. Kliknięcie przycisku **Zaawansowane** umożliwi skonfigurowanie ustawień połączenia z Serwerem administracyjnym (patrz rysunek poniżej).

   W celu nawiązania połączenia z Serwerem administracyjnym poprzez port inny niż domyślny, w polu **Adres Serwera administracyjnego** należy wprowadzić wartość w formacie <Nazwa Serwera administracyjnego>:<Numer portu>.

   Użytkownicy, którzy nie posiadają uprawnień do **Odczytu**, nie będą mieli dostępu do Serwera administracyjnego.



Nawiązywanie połączenia z Serwerem administracyjnym

4. Aby zakończyć przełączanie pomiędzy Serwerami, kliknij przycisk **OK**.

   Po podłączeniu Serwera administracyjnego, w drzewie konsoli zaktualizowane zostanie drzewo folderów odpowiedniego węzła.

Uprawnienia dostępu do Serwera administracyjnego i jego obiektów

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

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

- Jeśli aplikacja jest instalowana z poziomu konta użytkownika znajdującego się w domenie, grupy są tworzone na Serwerze administracyjnym i w domenie zawierającej Serwer administracyjny.
- Jeśli aplikacja jest instalowana z poziomu konta systemowego, grupy są tworzone jedynie na Serwerze administracyjnym.

Możesz przeglądać grupy **KLAdmins** i **KLOperators** oraz modyfikować uprawnienia dostępu użytkowników należących do grup **KLAdmins** i **KLOperators**, korzystając ze standardowych narzędzi administracyjnych systemu operacyjnego.

Grupa **KLAdmins** ma wszystkie uprawnienia dostępu, a grupa **KLOperators** ma jedynie uprawnienia Odczytu i Wykonywania. Uprawnienia nadane grupie **KLAdmins** są zablokowane.

Użytkownicy należący do grupy **KLAdmins** są nazywani *administratorami Kaspersky Security Center*, użytkownicy z grupy **KLOperators** są zwani *operatorami Kaspersky Security Center*.

Oprócz użytkowników z grupy **KLAdmins**, uprawnienia administratora Kaspersky Security Center są nadawane lokalnym administratorom urządzeń, na których zainstalowano Serwer administracyjny.

Możesz wykluczyć lokalnych administratorów z listy użytkowników, którzy posiadają uprawnienia administratora Kaspersky Security Center.

Wszystkie działania rozpoczęte przez administratorów Kaspersky Security Center zostaną wykonane przy użyciu uprawnień konta Serwera administracyjnego.

Dla każdego Serwera administracyjnego w sieci można utworzyć indywidualną grupę **KLAdmins**; będzie ona posiadać uprawnienia do pracy tylko z tym Serwerem administracyjnym.

Jeśli urządzenia należące do tej samej domeny znajdują się w grupach administracyjnych różnych Serwerów administracyjnych, wówczas administrator domeny jest administratorem Kaspersky Security Center dla wszystkich grup. Grupa **KLAdmins** jest wspólna dla tych grup administracyjnych; tworzona jest podczas instalacji pierwszego Serwera administracyjnego. Wszystkie działania podejmowane przez administratora Kaspersky Security Center są wykonywane przy pomocy uprawnień dostępu Serwera administracyjnego, dla którego rozpoczęto te działania.

Po zainstalowaniu aplikacji, administrator Kaspersky Security Center może:

- Modyfikować uprawnienia nadane grupom **KLOperators**.
- Nadawać uprawnienia dostępu do funkcji Kaspersky Security Center innym grupom użytkowników i pojedynczym użytkownikom zarejestrowanym na stacji roboczej administratora.
- Przydzielać uprawnienia dostępu każdej grupie administracyjnej.

Administrator Kaspersky Security Center może przydzielić uprawnienia dostępu do każdej grupy administracyjnej lub do innych obiektów Serwera administracyjnego w sekcji **Zabezpieczenia**, w oknie właściwości wybranego obiektu.

Możesz śledzić aktywność użytkowników przy pomocy wpisów dotyczących zdarzeń, które wystąpiły w trakcie pracy Serwera administracyjnego. Wpisy dotyczące zdarzeń są wyświetlane w węźle **Serwer administracyjny**, na zakładce **Zdarzenia**. Priorytetem tych zdarzeń jest **Informacja o zdarzeniach**, a typy zdarzeń rozpoczynają się od "**Audyt**".

Warunki połączenia z Serwerem administracyjnym przez internet

Jeżeli Serwer administracyjny jest zdalny (znajduje się poza siecią firmową), urządzenia klienckie mogą łączyć się z nim przez internet.

Aby urządzenia klienckie łączyły się z Serwerem administracyjnym przez Internet, muszą być spełnione następujące warunki:

- Zdalny Serwer administracyjny musi posiadać zewnętrzny adres IP, a port dla ruchu przychodzącego o numerze 13000 musi pozostać otwarty (dla połączenia z Agentami sieciowymi). Zalecane jest także otwarcie portu UDP o numerze 13000 (do odbierania powiadomień o zamknięciu urządzeń).
- Agenty sieciowe powinny zostać zainstalowane na urządzeniach.
- Podczas instalacji Agenta sieciowego na urządzeniach powinieneś określić zewnętrzny adres IP zdalnego Serwera administracyjnego. Jeżeli do instalacji wykorzystywany jest pakiet instalacyjny, zewnętrzny adres IP jest określany ręcznie we właściwościach tego pakietu instalacyjnego, na zakładce **Ustawienia**.
- Aby użyć zdalnego Serwera administracyjnego do zarządzania aplikacjami i zadaniami dla urządzenia, w oknie właściwości tego urządzenia, w sekcji **Ogólny** zaznacz pole **Nie odłączaj od Serwera administracyjnego**. Po zaznaczeniu tego pola, należy zaczekać, aż Serwer administracyjny zsynchronizuje się ze zdalnym urządzeniem. Liczba urządzeń klienckich mających stałe połączenie z Serwerem administracyjnym nie może przekraczać 300.

Aby zwiększyć wydajność zadań zainicjowanych przez zdalny Serwer administracyjny, możesz otworzyć na urządzeniu port o numerze 15000. W tym przypadku, aby uruchomić zadanie, Serwer administracyjny wysyła specjalny pakiet do Agenta sieciowego przez port 15000, bez oczekiwania na zakończenie synchronizacji z urządzeniem.

Nawiązywanie szyfrowanego połączenia z Serwerem administracyjnym

Wymiana danych między urządzeniami klienckimi a Serwerem administracyjnym, jak również połączenia Konsoli administracyjnej z Serwerem administracyjnym, może być przeprowadzana z użyciem protokołu TLS (Transport Layer Security). Protokół TLS może identyfikować współdziałające strony, szyfrować przesyłane dane oraz chronić je przed modyfikacją podczas transferu. Protokół TLS używa kluczy publicznych do autoryzowania współdziałających stron oraz szyfrowania danych.

Autoryzacja Serwera administracyjnego po podłączeniu urządzenia

Podczas pierwszego łączenia urządzenia klienckiego z Serwerem administracyjnym Agent sieciowy na urządzeniu pobiera certyfikat Serwera administracyjnego i zapisuje go lokalnie.

Jeśli instalujesz Agenta sieciowego lokalnie na urządzeniu, możesz ręcznie wybrać certyfikat Serwera administracyjnego.

Pobrana kopia certyfikatu jest używana do weryfikowania praw i przyzwoleń Serwera administracyjnego podczas kolejnych połączeń.

W trakcie następnych sesji Agent sieciowy będzie żądał certyfikatu Serwera administracyjnego przy każdym połączeniu urządzenia z Serwerem administracyjnym i będzie go porównywał z lokalną kopią. W przypadku, gdy obie kopie nie będą do siebie pasowały, urządzenie nie uzyska pozwolenia na dostęp do Serwera administracyjnego.

Autoryzacja Serwera administracyjnego podczas podłączania Konsoli administracyjnej

Podczas pierwszego połączenia z Serwerem administracyjnym Konsola administracyjna żąda certyfikatu Serwera administracyjnego i zapisuje go lokalnie na stacji roboczej administratora. Następnie, przy każdej próbie połączenia Konsoli administracyjnej z tym Serwerem administracyjnym, Serwer administracyjny zostanie zidentyfikowany na podstawie kopii certyfikatu.

Jeśli certyfikat Serwera administracyjnego nie odpowiada kopii przechowywanej na stacji roboczej administratora, Konsola administracyjna wyświetli pytanie o potwierdzenie nawiązania połączenia z Serwerem administracyjnym o określonej nazwie i pobranie nowego certyfikatu. Po nawiązaniu połączenia Konsola administracyjna zapisuje kopię nowego certyfikatu Serwera administracyjnego, która będzie wykorzystywana do identyfikowania Serwera administracyjnego w przyszłości.

Konfigurowanie listy dozwolonych adresów IP do łączenia się z Serwerem administracyjnym

Domyślnie użytkownicy mogą logować się do Kaspersky Security Center na dowolnym urządzeniu, na którym można otworzyć konsolę Kaspersky Security Center Web Console (zwaną dalej Web Console) lub konsolę administracyjną opartą na MMC. Możesz jednak skonfigurować serwer administracyjny tak, aby użytkownicy mogli łączyć się z nim tylko z urządzeń o dozwolonych adresach IP. W takim przypadku, nawet jeśli intruz ukradnie konto Kaspersky Security Center, nie będzie mógł zalogować się do Kaspersky Security Center, ponieważ adres IP urządzenia intruza nie znajduje się na liście zezwolonych.

Adres IP jest sprawdzany, gdy użytkownik loguje się do Kaspersky Security Center lub uruchamia aplikację, która współdziała z serwerem administracyjnym poprzez Kaspersky Security Center OpenAPI. W tym momencie urządzenie użytkownika próbuje nawiązać połączenie z Serwerem administracyjnym. Jeśli adresu IP urządzenia nie ma na liście dozwolonych, wystąpi błąd uwierzytelniania, a zdarzenie KLAUD_EV_SERVERCONNECT powiadamia, że połączenie z serwerem administracyjnym nie zostało nawiązane.

Wymagania dotyczące listy dozwolonych adresów IP

Adresy IP są weryfikowane tylko wtedy, gdy następujące aplikacje próbują połączyć się z serwerem administracyjnym:

- Web Console Server

  Jeśli logujesz się do Web Console na jednym urządzeniu, a serwer Web Console jest zainstalowany na innym, możesz skonfigurować zaporę sieciową na urządzeniu, na którym zainstalowano serwer konsoli internetowej, przy użyciu standardowych środków systemu operacyjnego. Następnie, jeśli ktoś spróbuje zalogować się do Web Console, zapora sieciowa pomoże zapobiec ingerencji intruzów.

- Konsola administracyjna

- Aplikacje współpracujące z serwerem administracyjnym za pośrednictwem obiektów automatyzacji klakaut

- Aplikacje współpracujące z serwerem administracyjnym za pośrednictwem interfejsu OpenAPI, takie jak Kaspersky Anti Targeted Attack Platform lub Kaspersky Security for Virtualization

Dlatego należy podać adresy urządzeń, na których zainstalowane są wymienione powyżej aplikacje.

Możesz ustawić adresy IPv4 i IPv6. Nie możesz określić zakresów adresów IP.

Jak ustanowić listę dozwolonych adresów IP

Jeśli wcześniej nie ustawiono listy dozwolonych, postępuj zgodnie z poniższymi instrukcjami.

W celu ustanowienia listy dozwolonych adresów IP do logowania się do Kaspersky Security Center:

1. Na urządzeniu serwera administracyjnego uruchom wiersz poleceń na koncie z uprawnieniami administratora.
2. Zmień bieżący katalog na folder instalacyjny Kaspersky Security Center (zwykle <dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Wpisz następujące polecenie, korzystając z uprawnień administratora:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<adresy IP>" -t s`

   Określ adresy IP, które spełniają powyższe wymagania. Wiele adresów IP należy oddzielać średnikami.

   Przykład — jak zezwolić tylko jednemu urządzeniu na łączenie się z serwerem administracyjnym:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Przykład — jak zezwolić wielu urządzeniom na łączenie się z serwerem administracyjnym:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`
4. Uruchom ponownie usługę Serwera administracyjnego.

Możesz dowiedzieć się, czy pomyślnie skonfigurowano listę dozwolonych adresów IP w dzienniku zdarzeń aplikacji Kaspersky na serwerze administracyjnym.

Jak zmienić listę dozwolonych adresów IP

Listę dozwolonych adresów można zmienić tak samo, jak podczas jej tworzenia. W tym celu uruchom to samo polecenie i określ nową listę dozwolonych adresów:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<adresy IP>" -t s
```

Jeśli chcesz usunąć niektóre adresy IP z listy dozwolonych, przepisz je. Na przykład, lista dozwolonych zawiera następujące adresy IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. Chcesz usunąć adres IP 198.51.100.0. Aby to zrobić, wpisz następujące polecenie w wierszu polecenia:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Nie zapomnij ponownie uruchomić usługi serwera administracyjnego.

Jak zresetować skonfigurowaną listę dozwolonych adresów IP

Aby zresetować już skonfigurowaną listę dozwolonych adresów IP:

1. Wpisz następujące polecenie w wierszu polecenia, korzystając z uprawnień administratora:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Uruchom ponownie usługę Serwera administracyjnego.

Następnie adresy IP nie będą już weryfikowane.

Użycie narzędzia klscflag do zamknięcia portu 13291

Port 13291 na serwerze administracyjnym jest używany do odbierania połączeń z konsoli administracyjnych. Ten port jest domyślnie otwarty. Jeśli nie chcesz używać konsoli administracyjnej opartej na MMC ani narzędzia klakaut, możesz zamknąć ten port za pomocą narzędzia klscflag. To narzędzie zmienia wartość parametru KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Aby zamknąć port 13291:

1. Wykonaj następujące polecenie w wierszu poleceń:
   `klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`

2. Uruchom ponownie usługę Serwera administracyjnego Kaspersky Security Center.

Port 13291 jest zamknięty.

Aby sprawdzić, czy port 13291 został pomyślnie zamknięty:

Wykonaj następujące polecenie w wierszu poleceń:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

To polecenie zwraca następujący wynik:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

Wartość `false` oznacza, że port jest zamknięty. W przeciwnym razie wyświetlana jest wartość `true`.

Odłączanie od Serwera administracyjnego

W celu odłączenia się od Serwera administracyjnego:

1. W drzewie konsoli wybierz węzeł odpowiadający Serwerowi administracyjnemu, który ma zostać odłączony.

2. Z menu kontekstowego węzła wybierz **Odłącz od Serwera administracyjnego**.

Dodawanie Serwera administracyjnego do drzewa konsoli

W celu dodania Serwera administracyjnego do drzewa konsoli:

1. W oknie głównym Kaspersky Security Center, w drzewie konsoli wybierz węzeł **Kaspersky Security Center**.

2. Z menu kontekstowego węzła wybierz **Nowy** → **Serwer administracyjny**.

Węzeł **Serwer administracyjny - <Nazwa urządzenia> (Niepołączony)** zostanie utworzony w drzewie konsoli, z której będziesz mógł połączyć się z dowolnym Serwerem administracyjnym zainstalowanym w sieci.

Usuwanie Serwera administracyjnego z drzewa konsoli

W celu usunięcia Serwera administracyjnego z drzewa konsoli:

1. W drzewie konsoli wybierz węzeł odpowiadający Serwerowi administracyjnemu, który ma zostać usunięty.
2. Z menu kontekstowego węzła wybierz **Usuń**.

Dodawanie wirtualnego Serwera administracyjnego do drzewa konsoli

W celu dodania wirtualnego Serwera administracyjnego do drzewa konsoli:

1. W drzewie konsoli należy wybrać węzeł z nazwą Serwera administracyjnego, dla którego chcesz utworzyć wirtualny Serwer administracyjny.
2. W węźle Serwera administracyjnego wybierz folder **Serwery administracyjne**.
3. W obszarze roboczym folderu **Serwery administracyjne** kliknij odnośnik **Dodaj wirtualny Serwer administracyjny**.

   Zostanie uruchomiony Kreator tworzenia nowego wirtualnego Serwera administracyjnego.
4. W oknie **Nazwa wirtualnego Serwera administracyjnego** określ nazwę tworzonego wirtualnego Serwera administracyjnego.

   Nazwa wirtualnego Serwera administracyjnego nie może zawierać więcej niż 255 znaków oraz nie może zawierać żadnych znaków specjalnych (takich jak "*<>?\:|).
5. W oknie **Wprowadzanie adresu połączenia urządzenia z wirtualnym Serwerem administracyjnym** określ adres połączenia urządzenia

   Adres połączenia wirtualnego Serwera administracyjnego to adres sieciowy, poprzez który urządzenia będą nawiązywać połączenie z tym Serwerem. Adres połączenia posiada dwie części: adres sieciowy fizycznego Serwera administracyjnego oraz nazwę wirtualnego Serwera administracyjnego, oddzielone ukośnikiem. Nazwa wirtualnego Serwera administracyjnego zostanie zastąpiona automatycznie. Określony adres będzie używany na wirtualnym Serwerze administracyjnym jako domyślny adres w pakietach instalacyjnych Agenta sieciowego.
6. W oknie **Utwórz konto administratora wirtualnego Serwera administracyjnego** wskaż użytkownika z listy, który będzie administratorem wirtualnego Serwera administracyjnego, lub dodaj nowe konto administratora, klikając przycisk **Utwórz**.

   Możesz określić kilka kont.

W drzewie konsoli tworzony jest węzeł o nazwie **Serwer administracyjny <Nazwa wirtualnego Serwera administracyjnego>**.

Zmienianie konta usługi Serwera administracyjnego. Narzędzie klsrvswch

Jeżeli chcesz zmienić konto usługi Serwera administracyjnego ustawione podczas instalacji Kaspersky Security Center, możesz użyć narzędzia klsrvswch, zaprojektowanego do zmieniania konta Serwera administracyjnego.

Podczas instalacji Kaspersky Security Center narzędzie jest automatycznie kopiowane do folderu instalacyjnego aplikacji.

Liczba uruchomień narzędzia jest właściwie nieograniczona.

Narzędzie klsrvswch umożliwia zmianę typu konta. Na przykład, jeśli korzystasz z konta lokalnego, możesz zmienić je na konto domenowe lub na zarządzane konto usługi (i odwrotnie). Narzędzie klsrvswch nie pozwala na zmianę typu konta na konto usługi zarządzane przez grupę (gMSA).

Windows Vista i późniejsze wersje systemu Windows nie pozwalają na użycie konta SystemLokalny dla Serwera administracyjnego. W tych wersjach systemu Windows opcja **Konto SystemLokalny** jest nieaktywna.

W celu zmiany konta usługi Serwera administracyjnego na konto domeny:

1. Z folderu instalacyjnego Kaspersky Security Center użyj narzędzia klsrvswch.

   Akcja ta uruchamia również Kreator modyfikacji konta usługi Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

2. W oknie **Konto usługi Serwera administracyjnego** wybierz **Konto SystemLokalny**.

Po zakończeniu działania kreatora, zostanie zmienione konto Serwera administracyjnego. Serwer administracyjny rozpocznie pracę przy użyciu *Konto SystemLokalny* i użyje jego danych uwierzytelniających.

Do poprawnego działania Kaspersky Security Center wymagane jest, aby konto używane do uruchamiania Serwera administracyjnego posiadało uprawnienia administratora do zasobu, w którym przechowywana jest baza danych Serwera administracyjnego.

W celu zmiany konta usługi Serwera administracyjnego na konto użytkownika lub konto zarządzanej usługi:

1. Z folderu instalacyjnego Kaspersky Security Center użyj narzędzia klsrvswch.

   Akcja ta uruchamia również Kreator modyfikacji konta usługi Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora.

2. W oknie **Konto usługi Serwera administracyjnego** wybierz **Konto niestandardowe**.

3. Kliknij przycisk **Znajdź teraz**.

   Zostanie otwarte okno **Wybierz użytkownika**.

4. W otwartym oknie **Wybierz użytkownika** kliknij przycisk **Typy obiektów**.

5. Na liście typów obiektów wybierz **Użytkownicy** (jeśli chcesz konto użytkownika) lub **Konta usługi** (jeśli chcesz zarządzane konto usługi) i kliknij **OK**.

6. W polu nazwy obiektu wpisz nazwę konta lub część nazwy i kliknij **Sprawdź nazwy**.

7. Na liście pasujących nazw wybierz żądaną nazwę, a następnie kliknij **OK**.

8. Jeśli wybrałeś **Konta usługi**, w oknie **Hasło do konta** pozostaw pola **Hasło** i **Potwierdź hasło** puste. Jeśli wybrałeś **Użytkownicy**, wprowadź nowe hasło dla użytkownika i potwierdź je.

Konto usługi Serwera administracyjnego zostanie zmienione na konto, które wybrałeś.

Podczas korzystania z Microsoft SQL Server w trybie uwierzytelniania konta użytkownika przy użyciu narzędzi Microsoft Windows, nadane muszą zostać uprawnienia dostępu do bazy danych. Baza danych Kaspersky Security Center powinna należeć do tego konta użytkownika. Domyślnie używany jest schemat dbo.

Zmiana poświadczeń DBMS

Czasami może zajść potrzeba zmiany poświadczeń DBMS, na przykład w celu wykonania rotacji poświadczeń ze względów bezpieczeństwa.

W celu zmiany poświadczeń DBMS w środowisku Windows przy użyciu klsrvswch.exe:

1. Uruchom narzędzie klsrvswch znajdujące się w folderze instalacyjnym programu Kaspersky Security Center.
2. Kliknij przycisk **Dalej** kreatora, aż dojdziesz do kroku **Zmień poświadczenia dostępu do DBMS**.
3. W tym kroku **Zmień poświadczenia dostępu do DBMS** wykonaj następujące czynności:
   - Wybierz opcję **Zastosuj nowe poświadczenia**.
   - Podaj nową nazwę konta w polu **Konto**.
   - Podaj nowe hasło do konta w polu **Hasło**.
   - Określ nowe hasło w polu **Potwierdź hasło**.

   Powinieneś określić poświadczenia konta, które istnieje w DBMS.
4. Kliknij przycisk **Dalej**.

Po zakończeniu pracy kreatora poświadczenia DBMS zostają zmienione.

Rozwiązywanie problemów z węzłami Serwera administracyjnego

Drzewo konsoli w lewej części Konsoli administracyjnej zawiera węzły Serwerów administracyjnych. W drzewie konsoli możesz dodać tyle Serwerów administracyjnych, ile potrzebujesz.

Lista węzłów Serwerów administracyjnych w drzewie konsoli jest przechowywana w kopii pliku .msc w tle przy użyciu konsoli Microsoft Management Console. Kopia w tle tego pliku znajduje się w folderze %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ na urządzeniu, na którym jest zainstalowana Konsola administracyjna. Dla każdego węzła Serwera administracyjnego plik zawiera następujące informacje:

- Adres Serwera administracyjnego
- Numer portu
- Czy TLS jest używany

Ten parametr zależy od numeru portu, użytego do nawiązania połączenia między Konsolą administracyjną a Serwerem administracyjnym.

- Nazwa użytkownika
- Certyfikatu Serwera administracyjnego

Rozwiązywanie problemów

Jeśli Konsola administracyjna nawiąże połączenie z Serwerem administracyjnym, certyfikat przechowywany lokalnie jest porównywany do certyfikatu Serwera administracyjnego. Jeśli certyfikaty nie pasują do siebie, Konsola administracyjna wygeneruje błąd. Na przykład, niedopasowanie certyfikatów może wystąpić, gdy zastąpisz certyfikat Serwera administracyjnego. W tym przypadku, w konsoli utwórz ponownie węzeł Serwera administracyjnego.

W celu ponownego utworzenia węzła Serwera administracyjnego:

1. Zamknij okno Konsoli administracyjnej Kaspersky Security Center.
2. Usuń plik w Kaspersky Security Center 14.2 w %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Uruchom Konsolę administracyjną Kaspersky Security Center.

   Zostanie wyświetlone pytanie o nawiązanie połączenia z Serwerem administracyjnym i zaakceptowanie jego istniejącego certyfikatu.
4. Wykonaj jedną z poniższych czynności:
   - Zaakceptuj istniejący certyfikat, klikając przycisk **Tak**.
   - Aby określić swój certyfikat, kliknij przycisk **Nie**, a następnie odszukaj plik certyfikatu, który zostanie użyty do autoryzacji na Serwerze administracyjnym.

Problem z certyfikatem zostanie rozwiązany. Do nawiązania połączenia z Serwerem administracyjnym możesz użyć Konsoli administracyjnej.

Przeglądanie i modyfikowanie ustawień Serwera administracyjnego

Ustawienia Serwera administracyjnego można dostosować w oknie właściwości tego Serwera.

W celu otwarcia okna Właściwości: Serwer administracyjny:

Z menu kontekstowego węzła Serwera administracyjnego w drzewie konsoli wybierz element **Właściwości**.

Dostosowywanie ogólnych ustawień Serwera administracyjnego

Ogólne ustawienia Serwera administracyjnego można dostosować w sekcjach **Ogólny**, **Ustawienia połączenia z Serwerem administracyjnym**, **Repozytorium zdarzeń** i **Zabezpieczenia**, dostępnych w oknie właściwości Serwera administracyjnego.

Sekcja **Zabezpieczenia** nie jest wyświetlana w oknie właściwości Serwera administracyjnego, jeśli wyświetlanie zostało wyłączone w interfejsie Konsoli administracyjnej.

*W celu włączenia wyświetlania sekcji **Zabezpieczenia** w Konsoli administracyjnej:*

1. W drzewie konsoli wybierz Serwer administracyjny, którego potrzebujesz.
2. W menu **Widok** okna głównego aplikacji wybierz **Konfiguruj interfejs**.
3. W otwartym oknie **Konfiguruj interfejs** zaznacz pole **Wyświetl sekcje ustawień zabezpieczeń** i kliknij **OK**.
4. W oknie z wiadomością aplikacji kliknij **OK**.

Sekcja **Zabezpieczenia** będzie wyświetlana w oknie właściwości Serwera administracyjnego.

Ustawienia interfejsu Konsoli administracyjnej

Możesz dostosować ustawienia interfejsu Konsoli administracyjnej do wyświetlania lub ukrywania kontrolek interfejsu użytkownika związanych z następującymi funkcjami:

- Zarządzanie lukami i poprawkami
- Szyfrowanie i ochrona danych
- Ustawienia kontroli węzła końcowego
- Zarządzanie urządzeniami mobilnymi
- Podrzędne Serwery administracyjne
- Sekcje Ustawienia zabezpieczeń

W celu skonfigurowania ustawień interfejsu Konsoli administracyjnej:

1. W drzewie konsoli wybierz Serwer administracyjny, którego potrzebujesz.
2. W menu **Widok** okna głównego aplikacji wybierz **Konfiguruj interfejs**.
3. W otwartym oknie **Konfiguruj interfejs** zaznacz pola obok funkcji, które mają być wyświetlane, a następnie kliknij **OK**.
4. W oknie z wiadomością aplikacji kliknij **OK**.

Wybrane funkcje zostaną wyświetlone w interfejsie Konsoli administracyjnej.

Przetwarzanie i przechowywanie zdarzeń na Serwerze administracyjnym

Informacje o zdarzeniach, występujących podczas działania aplikacji, oraz o zarządzanych urządzeniach są wyświetlane w bazie danych Serwera administracyjnego. Każdemu zdarzeniu przypisywany jest określony typ i priorytet (*Zdarzenie krytyczne*, *Błąd funkcjonalny*, *Ostrzeżenie* lub *Informacja*). W zależności od warunków, przez które pojawiło się zdarzenie, do zdarzeń tego samego typu aplikacja może przypisywać różne priorytety.

Typy i priorytety przypisane do zdarzeń można sprawdzić w sekcji **Konfiguracja zdarzenia** okna właściwości Serwera administracyjnego. W sekcji **Konfiguracja zdarzenia** możesz także skonfigurować przetwarzanie każdego zdarzenia przez Serwer administracyjny:

- Rejestrację zdarzeń na Serwerze administracyjnym i w raporcie zdarzeń systemu operacyjnego na urządzeniu i na Serwerze administracyjnym.

- Metodę używaną do informowania administratora o zdarzeniu (na przykład, wiadomość SMS lub e-mail).

W sekcji **Repozytorium zdarzeń** okna właściwości Serwera administracyjnego możesz zmodyfikować ustawienia przechowywania zdarzeń w bazie danych Serwera administracyjnego, ograniczając liczbę wpisów zdarzeń i czas przechowywania wpisów. Jeśli określisz maksymalną liczbę zdarzeń, aplikacja oblicza przybliżoną ilość miejsca przechowywania, wymaganą dla określonej liczby. Możesz użyć tego przybliżonego obliczenia do oszacowania wystarczającej ilości wolnego miejsca na dysku, aby uniknąć przepełnienia bazy danych. Domyślna pojemność bazy danych Serwera administracyjnego wynosi 400 000 zdarzeń. Maksymalną dozwoloną pojemnością bazy danych jest 45 milionów zdarzeń.

Jeśli liczba zdarzeń w bazie danych osiągnie maksymalną wartość określoną przez administratora, aplikacja usunie najstarsze zdarzenia i zastąpi je nowymi. Jeśli Serwer administracyjny usuwa starsze zdarzenia, nie może zapisywać nowych zdarzeń do bazy danych. W tym czasie informacje o odrzuconych zdarzeniach są zapisywane w dzienniku zdarzeń aplikacji Kaspersky. Nowe zdarzenia zostają zakolejkowane, a następnie zapisane do bazy danych po zakończeniu operacji usuwania.

Możesz zmienić ustawienia dowolnego zadania zapisywać zdarzenia związane z postępem zadania lub zapisywać tylko wyniki wykonania zadania. Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Przeglądanie raportów połączeń z Serwerem administracyjnym

Historia połączeń i prób nawiązania połączenia z Serwerem administracyjnym podczas jego działania może zostać zapisana w pliku raportu. Informacje w pliku umożliwiają śledzenie nie tylko połączeń w obrębie infrastruktury sieci, ale także nieautoryzowanych prób uzyskania dostępu do Serwera administracyjnego.

W celu zapisania zdarzeń nawiązania połączenia z Serwerem administracyjnym:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz włączyć zapisywanie zdarzeń połączenia.

2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

3. W otwartym oknie właściwości, w sekcji **Ustawienia połączenia z Serwerem administracyjnym** wybierz podsekcję **Porty połączenia**.

4. Włącz opcję **Zapisuj zdarzenia połączenia z Serwerem administracyjnym**.

5. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.

Wszystkie dalsze zdarzenia przychodzących połączeń z Serwerem administracyjnym, wyniki autoryzacji i błędy SSL zostaną zapisane do pliku %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Kontrola epidemii wirusów

Kaspersky Security Center umożliwia szybkie reagowanie na pojawiające się zagrożenia epidemiami wirusów. Ryzyko wystąpienia epidemii wirusów jest szacowane w oparciu o kontrolę aktywności wirusów na urządzeniach.

W sekcji **Epidemia wirusa**, dostępnej w oknie właściwości Serwera administracyjnego, możesz skonfigurować reguły oceny dla zagrożeń epidemią wirusów i akcje wykonywane w razie epidemii.

Możesz określić procedurę powiadamiania dla zdarzenia *Epidemia wirusa* w sekcji **Konfiguracja zdarzenia** okna właściwości Serwera administracyjnego, w oknie właściwości zdarzenia *Epidemia wirusa*.

Zdarzenie *Epidemia wirusa* jest generowane w przypadku wykrycia zdarzeń *Wykryto szkodliwy obiekt* w trakcie działania aplikacji zabezpieczających. Dlatego też należy zapisywać informacje o wszystkich zdarzeniach *Wykryto szkodliwy obiekt* na Serwerze administracyjnym, aby móc rozpoznać epidemie wirusów.

Możesz określić ustawienia zapisywania informacji o każdym zdarzeniu *Wykryto szkodliwy obiekt* w profilach aplikacji zabezpieczających.

Podczas zliczania zdarzeń *Wykryto szkodliwy obiekt* pod uwagę brane są wyłącznie informacje z urządzeń głównego Serwera administracyjnego. Informacje od podrzędnych Serwerów administracyjnych nie są brane pod uwagę. Ustawienia zdarzenia *Epidemia wirusa* są konfigurowane indywidualnie dla każdego Serwera podrzędnego.

Ograniczanie ruchu sieciowego

Aby zmniejszyć ruch sieciowy w obrębie sieci, aplikacja posiada opcję ograniczania prędkości przesyłania danych na Serwer administracyjny z określonych zakresów IP i podsieci IP.

Reguły ograniczania ruchu sieciowego można utworzyć i skonfigurować w sekcji **Ruch sieciowy** okna właściwości Serwera administracyjnego.

W celu utworzenia reguły ograniczania ruchu sieciowego:

1. W drzewie konsoli należy wybrać węzeł z nazwą Serwera administracyjnego, dla którego chcesz utworzyć regułę ograniczenia ruchu sieciowego.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Ruch sieciowy**.
4. Kliknij przycisk **Dodaj**.
5. W sekcji **Nowa reguła** określ następujące ustawienia:

   W sekcji **Zakres IP, dla którego ograniczany jest ruch sieciowy** wybierz metodę, która będzie używana do określenia podsieci lub zakresu, dla którego przesyłanie danych będzie ograniczone, a następnie wprowadź wartości ustawień dla wybranej metody. Wybierz jedną z następujących metod:

   - **Określ zakres poprzez adres oraz maskę sieci**

     Ruch sieciowy jest ograniczony na podstawie ustawień podsieci. Określ adres podsieci i maskę podsieci do określania zakresu, w którym ruch sieciowy będzie ograniczony.

     Możesz także kliknąć **Przeglądaj**, aby dodać podsieci z globalnej listy podsieci.

   - **Określ zakres podając adres początkowy i końcowy**

     Ruch sieciowy jest ograniczony w oparciu o zakres adresów IP. Określ zakres adresów IP w polach **Adres początkowy** oraz **Adres końcowy**.

     Opcja ta jest wybrana domyślnie.

W sekcji **Ograniczenie ruchu sieciowego** możesz dostosować następujące restrykcyjne ustawienia współczynnika przesyłania danych:

- **Przedział czasu**

  Przedział czasu, w trakcie którego zostanie zastosowane ograniczenie ruchu sieciowego. W polach do wprowadzania danych można określić granice przedziału czasu.

- **Ograniczenie (KB/s)**

  Maksymalna łączna szybkość transferu danych przychodzących i wychodzących Serwera administracyjnego. Ograniczenie ruchu sieciowego będzie stosowane tylko w obrębie przedziału czasu określonego w polu **Przedział czasu**.

- **Ogranicz ruch w pozostałym czasie (KB/s)**

  Ruch sieciowy będzie ograniczony nie tylko w czasie określonym w polu **Przedział czasu**, ale także w pozostałym czasie.

  Domyślnie pole to nie jest zaznaczone. Wartość tego pola nie może odpowiadać wartości pola **Ograniczenie (KB/s)**.

Przede wszystkim, reguły ograniczenia ruchu sieciowego wpływają na przesyłanie plików. Te reguły nie są stosowane do ruchu sieciowego wygenerowanego przez synchronizację między Serwerem administracyjnym a Agentem sieciowym lub między głównym a podrzędnym Serwerem administracyjnym.

Konfigurowanie serwera sieciowego

Serwer sieciowy został zaprojektowany do publikowania autonomicznych pakietów instalacyjnych, profili iOS MDM oraz plików z folderu współdzielonego.

Możesz zdefiniować ustawienia łączenia serwera sieciowego z Serwerem administracyjnym oraz określić certyfikat serwera sieciowego w sekcji **Serwer WWW** okna właściwości Serwera administracyjnego.

Praca z użytkownikami wewnętrznymi

Konta *użytkowników wewnętrznych* są używane do pracy z wirtualnymi Serwerami administracyjnymi. Kaspersky Security Center nadaje wewnętrznym użytkownikom aplikacji uprawnienia rzeczywistych użytkowników.

Konta wewnętrznych użytkowników są tworzone i używane tylko w obrębie Kaspersky Security Center. Do systemu operacyjnego nie są przesyłane żadne dane dotyczące wewnętrznych użytkowników. Kaspersky Security Center autoryzuje wewnętrznych użytkowników.

Możesz skonfigurować konta użytkowników wewnętrznych w folderze **Konta użytkowników** drzewa konsoli.

Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego

Tworzenie kopii zapasowej ustawień Serwera administracyjnego i jego baz danych odbywa się przy użyciu zadania tworzenia kopii zapasowej oraz narzędzia klbackup. Kopia zapasowa zawiera wszystkie główne ustawienia i obiekty dotyczące Serwera administracyjnego, takie jak certyfikaty, klucze główne do szyfrowania dysków na zarządzanych urządzeniach, klucze dla różnych licencji, strukturę grup administracyjnych z całą ich zawartością, zadaniami, zasadami itd. Przy pomocy kopii zapasowej można przywrócić działanie Serwera administracyjnego tak szybko, jak to możliwe, poświęcając na to od kilkunastu minut do kilku godzin.

Jeśli nie ma dostępnej kopii zapasowej, błąd może doprowadzić do bezpowrotnej utraty certyfikatów i wszystkich ustawień Serwera administracyjnego. Będzie to wymagało przeprowadzenia konfiguracji Kaspersky Security Center od początku oraz ponownego zainstalowania Agenta sieciowego w sieci organizacji. Wszystkie klucze główne do szyfrowania dysków na zarządzanych urządzeniach zostaną utracone, co spowoduje ryzyko utraty zaszyfrowanych danych na urządzeniach z zainstalowanym programem Kaspersky Endpoint Security. Dlatego też nigdy nie rezygnuj z regularnego wykonywania kopii zapasowej Serwera administracyjnego przy użyciu standardowego zadania tworzenia kopii zapasowej.

Kreator wstępnej konfiguracji tworzy zadanie wykonywania kopii zapasowej dla ustawień Serwera administracyjnego i ustawia jego codzienne wykonywanie na godzinę 4:00. Kopie zapasowe są domyślnie zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskySC.

Jeśli serwer Microsoft SQL Server, zainstalowany na innym urządzeniu, jest używany jako DBMS, należy zmodyfikować zadanie tworzenia kopii zapasowej, określając jako folder do przechowywania kopii zapasowych ścieżkę UNC, która jest używana do zapisywania usługi Serwera administracyjnego oraz usługi SQL Server. To wymaganie, które nie jest oczywiste, wynika ze specyfiki specjalnej funkcji kopii zapasowej w systemie DBMS serwera Microsoft SQL Server.

Jeśli jako system DBMS używana jest lokalna instancja serwera Microsoft SQL Server, zalecane jest zapisanie kopii zapasowych na dedykowanym nośniku w celu zabezpieczenia ich przed uszkodzeniem wraz z Serwerem administracyjnym.

Ponieważ kopia zapasowa zawiera ważne dane, zadanie tworzenia kopii zapasowej oraz narzędzie klbackup oferują ochronę kopii zapasowej przy użyciu hasła. Domyślnie zadanie tworzenia kopii zapasowej wykonuje kopię zapasową z pustym hasłem. Hasło należy ustawić we właściwościach zadania tworzenia kopii zapasowej. Pominięcie tego wymagania doprowadza do sytuacji, w której wszystkie klucze certyfikatów Serwera administracyjnego, klucze dla licencji oraz klucze główne dla szyfrowania dysków na zarządzanych urządzeniach pozostaną niezaszyfrowane.

Oprócz regularnych kopii zapasowych, kopie zapasowe należy tworzyć także przed każdą znaczącą zmianą, w tym instalacją aktualizacji i łat Serwera administracyjnego.

Jeśli używasz Microsoft SQL Server jako DBMS, możesz zminimalizować rozmiar kopii zapasowych. W tym celu włącz opcję **Kompresuj kopię zapasową** w ustawieniach SQL Server.

Przywracanie kopii zapasowej odbywa się przy użyciu narzędzia klbackup na działającej instancji Serwera administracyjnego, który został właśnie zainstalowany i posiada tę samą wersję (lub nowszą), dla której kopia zapasowa została utworzona.

Instancja Serwera administracyjnego, na którym kopia zapasowa ma zostać przywrócona, musi korzystać z systemu DBMS tego samego typu (na przykład ten sam SQL Server lub MariaDB) i tej samej lub nowszej wersji. Wersja Serwera administracyjnego może być taka sama (z tą samą lub późniejszą łatą) lub nowsza.

Sekcja opisuje standardowe scenariusze przywracania ustawień i obiektów Serwera administracyjnego.

Używanie migawek systemu plików do skrócenia czasu tworzenia kopii zapasowej

W Kaspersky Security Center 14.2 czas bezczynności serwera administracyjnego w trakcie wykonywania kopii zapasowej został skrócony w porównaniu do wcześniejszych wersji. Co więcej, funkcja **Użyj migawki systemu plików do wykonania kopii zapasowej danych** została dodana do ustawień zadania. Ta funkcja zapewnia dodatkową redukcję czasu bezczynności przy użyciu narzędzia klbackup, które tworzy w tle kopię dysku podczas wykonywania kopii zapasowej (zajmuje to kilka sekund) i jednocześnie kopiuje bazę danych (najdłużej może to potrwać kilka minut). Jeśli narzędzie klbackup utworzy w tle kopię dysku oraz kopię bazy danych, ponownie umożliwi połączenie z Serwerem administracyjnym.

Funkcja tworzenia migawek systemu plików może być używana tylko wtedy, gdy spełnione są te dwa warunki:

- Folder współdzielony Serwera administracyjnego oraz folder %ALLUSERSPROFILE%\KasperskyLab znajdują się na tym samym dysku logicznym i są lokalne w odniesieniu do Serwera administracyjnego.
- Folder %ALLUSERSPROFILE%\KasperskyLab nie zawiera żadnych łączy symbolicznych, które zostały utworzone ręcznie.

Nie używaj tej funkcji, jeśli żaden z tych warunków nie może zostać spełniony. W tym przypadku, w odpowiedzi na jakąkolwiek próbę utworzenia migawki systemu plików aplikacja zwróci komunikat o błędzie.

Aby użyć funkcji, musisz posiadać konto, któremu nadano uprawnienie do tworzenia migawek dysku logicznego, na którym znajduje się folder %ALLUSERSPROFILE%. Należy pamiętać, że konto usługi Serwera administracyjnego nie posiada takiego uprawnienia.

W celu użycia funkcji tworzenia migawek systemu plików do skrócenia czasu tworzenia kopii zapasowej:

1. W sekcji **Zadania** wybierz zadanie tworzenia kopii zapasowej.
2. Z menu kontekstowego wybierz **Właściwości**.
3. W oknie właściwości zadania wybierz sekcję **Ustawienia**.
4. Zaznacz pole **Użyj migawki systemu plików do wykonania kopii zapasowej danych**.
5. W polach **Nazwa użytkownika** i **Hasło** wprowadź nazwę i hasło dla konta, któremu nadano uprawnienie do tworzenia migawek dysku logicznego, na którym znajduje się folder %ALLUSERSPROFILE%.
6. Kliknij **Zastosuj**.

Przy każdym kolejnym uruchomieniu zadania tworzenia kopii zapasowej narzędzie klbackup utworzy migawki systemu plików, skracając czas bezczynności Serwera administracyjnego podczas wykonywania zadania.

Urządzenie z zainstalowanym Serwerem administracyjnym nie działa

Jeśli urządzenie, na którym jest zainstalowany Serwer administracyjny, nie działa z powodu błędu, zalecane jest wykonanie następujących działań:

- Nowy Serwer administracyjny musi posiadać ten sam adres: nazwę NetBIOS, nazwę FQDN lub statyczny adres IP (w zależności od tego, co zostało ustawione podczas instalacji Agentów sieciowych).
- Zainstaluj Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.
- W menu **Start** uruchom narzędzie klbackup i wykonaj przywracanie.

Ustawienia Serwera administracyjnego lub bazy danych są uszkodzone

Jeżeli Serwer administracyjny nie działa ze względu na uszkodzone ustawienia lub bazę danych (na przykład, w wyniku przepięcia), zalecane jest użycie następujących scenariuszy:

1. Przeskanuj system plików na uszkodzonym urządzeniu.
2. Odinstaluj niedziałającą wersję Systemu operacyjnego.
3. Zainstaluj ponownie Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej (lub nowszej) wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.
4. Z poziomu menu **Start** uruchom narzędzie klbackup i przywróć kopię zapasową.

Zabronione jest przywracanie Serwera administracyjnego w sposób inny niż przy użyciu narzędzia klbackup.

Wszelkie próby przywrócenia Serwera administracyjnego przy użyciu oprogramowania firm trzecich doprowadzą do desynchronizacji danych na węzłach aplikacji Kaspersky Security Center i w konsekwencji - do niepoprawnego działania aplikacji.

Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego

Tworzenie kopii zapasowej danych umożliwia przeniesienie Serwera administracyjnego z jednego urządzenia na inne, bez utraty danych. Dzięki kopii zapasowej możesz przywrócić dane podczas przenoszenia bazy danych Serwera administracyjnego na inne urządzenie lub podczas aktualizacji do nowej wersji Kaspersky Security Center.

Pamiętaj, że nie są tworzone kopie zapasowe zainstalowanych wtyczek do zarządzania. Po przywróceniu danych Serwera administracyjnego z kopii zapasowej należy pobrać i ponownie zainstalować wtyczki dla zarządzanych aplikacji.

Możesz utworzyć kopię zapasową danych Serwera administracyjnego w jeden z następujących sposobów:

- Tworząc i uruchamiając zadanie wykonywania kopii zapasowej danych poprzez Konsolę administracyjną.
- Uruchamiając narzędzie klbackup na urządzeniu, na którym jest zainstalowany Serwer administracyjny. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Po zainstalowaniu Serwera administracyjnego, narzędzie jest umieszczane w katalogu głównym folderu docelowego, określonego podczas instalacji aplikacji.

W kopii zapasowej Serwera administracyjnego zapisywane są następujące dane:

- Baza danych Serwera administracyjnego (profile, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym).
- Informacje o konfiguracji struktury grup administracyjnych i urządzeń klienckich.
- Repozytorium pakietów dystrybucyjnych aplikacji przeznaczonych do zdalnego zainstalowania.
- Certyfikat Serwera administracyjnego.

Odzyskanie danych Serwera administracyjnego jest możliwe tylko przy użyciu narzędzia klbackup.

Tworzenie zadania wykonywania kopii zapasowej

Zadania kopii zapasowej są zadaniami Serwera administracyjnego i są tworzone podczas działania kreatora wstępnej konfiguracji. Jeśli zadanie kopii zapasowej utworzone przez Kreator wstępnej konfiguracji zostało usunięte, możesz je utworzyć ręcznie.

W celu utworzenia zadania kopii zapasowej danych Serwera administracyjnego:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Uruchom tworzenie zadania w jeden z następujących sposobów:
   - Wybierając **Nowe** → **Zadanie** w menu kontekstowym folderu **Zadania** w drzewie konsoli.
   - Kliknij przycisk **Utwórz zadanie** w obszarze roboczym.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora. W oknie **Wybierz typ zadania** wybierz typ zadania **Kopia zapasowa danych Serwera administracyjnego**.

Zadanie **Kopia zapasowa danych Serwera administracyjnego** może zostać utworzone tylko w jednej kopii. Jeśli dla Serwera administracyjnego już utworzono zadanie tworzenia kopii zapasowych danych Serwera administracyjnego, nie będzie wyświetlane w oknie wyboru typu zadania kreatora tworzenia zadania kopii zapasowej Serwera administracyjnego.

Narzędzie do tworzenia kopii zapasowej i odzyskiwania danych (klbackup)

Możesz utworzyć kopie danych Serwera administracyjnego w celu przechowywania kopii zapasowych oraz przyszłego ich odzyskania przy użyciu narzędzia klbackup stanowiącego część pakietu dystrybucyjnego Kaspersky Security Center.

Narzędzie klbackup można uruchomić w jednym z dwóch trybów:

- Interaktywnym
- Nieinteraktywnym

Tworzenie kopii zapasowej i przywracanie danych w trybie interaktywnym

W celu utworzenia kopii zapasowej danych Serwera administracyjnego w trybie interaktywnym:

1. Uruchom narzędzie klbackup znajdujące się w folderze instalacyjnym Kaspersky Security Center.

   Zostanie uruchomiony Kreator tworzenia kopii zapasowej i przywracania.
2. W pierwszym oknie kreatora wybierz **Wykonaj kopię zapasową danych Serwera administracyjnego**.

Jeśli wybierzesz opcję **Przywróć lub wykonaj kopię zapasową jedynie certyfikatu Serwera administracyjnego**, zostanie zapisana tylko kopia zapasowa certyfikatu Serwera administracyjnego.

Kliknij **Dalej**.

3. W kolejnym oknie Kreatora określ następujące opcje:

   - **Folder docelowy kopii zapasowej**
   - **Migracja do formatu MySQL/MariaDB**

     Włącz tę opcję, jeśli obecnie używasz SQL Server jako DBMS dla Serwera administracyjnego i chcesz przeprowadzić migrację danych z SQL Server do MySQL lub MariaDB DBMS. Kaspersky Security Center utworzy kopię zapasową kompatybilną z MySQL i MariaDB. Następnie możesz przywrócić dane z kopii zapasowej do MySQL lub MariaDB.

   - **Wykonaj migrację do formatu Azure**

     Włącz tę opcję, jeśli obecnie używasz SQL Server jako DBMS dla Serwera administracyjnego i chcesz przeprowadzić migrację danych z SQL Server do Azure SQL DBMS. Kaspersky Security Center utworzy kopię zapasową kompatybilną z Azure SQL. Następnie możesz przywrócić dane z kopii zapasowej do Azure SQL.

   - **Dołącz bieżącą datę i czas do nazwy folderu docelowego przechowującego kopie zapasowe**
   - **Hasło do kopii zapasowej**

4. Kliknij przycisk **Dalej**, aby uruchomić tworzenie kopii zapasowej.

5. Jeśli pracujesz z bazami danych w środowisku chmury, takim jak Amazon Web Services (AWS) lub Microsoft Azure, w oknie **Zaloguj się do magazynu online** wypełnij następujące pola:

   - Dla AWS:

     - **Nazwa komory S3**

       Nazwa komory S3, którą utworzyłeś dla Kopii zapasowej.

     - **Identyfikator klucza dostępu**

       Identyfikator klucza (sekwencja znaków alfanumerycznych) uzyskałeś podczas tworzenia konta użytkownika IAM do pracy z instancją magazynu komory S3.

       Pole jest dostępne, jeśli w komorze S3 wybrałeś bazę danych RDS.

     - **Tajny klucz**

Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

- Dla Microsoft Azure:
  - **Nazwa konta magazynu Azure**

    Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

  - **ID subskrypcji Azure**

    Subskrypcję utworzyłeś na portalu Azure.

  - **Hasło Azure**

    Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

    Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

  - **ID aplikacji Azure**

    Ten ID aplikacji utworzyłeś na portalu Azure.

    Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

  - **Nazwa serwera Azure SQL**

    Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

  - **Grupa zasobów serwera Azure SQL**

    Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

  - **Klucz dostępu do magazynu Azure**

    Dostępne we właściwościach Twojego konta magazynu, w sekcji Klucze dostępu. Możesz użyć dowolnego klucza (key1 lub key2).

W celu przywrócenia danych Serwera administracyjnego w trybie interaktywnym:

1. Uruchom narzędzie klbackup znajdujące się w folderze instalacyjnym Kaspersky Security Center. Uruchom narzędzie z tego samego konta, którego użyłeś do zainstalowania Serwera administracyjnego. Zalecamy

uruchomienie narzędzia na nowo zainstalowanym Serwerze administracyjnym.

Zostanie uruchomiony Kreator tworzenia kopii zapasowej i przywracania.

2. W pierwszym oknie kreatora wybierz **Przywróć dane Serwera administracyjnego**.

   Jeśli wybierzesz opcję **Przywróć lub wykonaj kopię zapasową jedynie certyfikatu Serwera administracyjnego**, certyfikat Serwer administracyjny zostanie tylko przywrócony.

   Kliknij **Dalej**.

3. W oknie **Przywróć ustawienia**:

   - Wskaż folder, który zawiera kopię zapasową danych Serwera administracyjnego.

     Jeśli pracujesz w środowisku chmury, takim jak AWS lub Azure, określ adres magazynu. Musisz się także upewnić, że plik nosi nazwę backup.zip.

   - Określ hasło, które zostało wprowadzone podczas tworzenia kopii zapasowej danych.

     Podczas przywracania danych powinieneś określić to samo hasło, które wprowadziłeś podczas tworzenia kopii zapasowej. Jeśli po utworzeniu kopii zapasowej ścieżka do folderu współdzielonego uległa zmianie, sprawdź działanie zadań wykorzystujących przywrócone dane (zadania przywracania i zadania zdalnej instalacji). Jeśli jest to konieczne, zmodyfikuj ustawienia tych zadań. Podczas przywracania danych z pliku kopii zapasowej nikt nie może mieć dostępu do folderu współdzielonego Serwera administracyjnego. Konto, z poziomu którego uruchamiane jest narzędzie klbackup, musi mieć pełen dostęp do folderu współdzielonego.

4. Kliknij przycisk **Dalej**, aby przywrócić dane.

Tworzenie kopii zapasowej i przywracanie danych w trybie nieinteraktywnym

W celu utworzenia kopii zapasowej lub odzyskania danych Serwera administracyjnego w trybie nieinteraktywnym:

Uruchom narzędzie klbackup z żądanym zestawem przełączników z poziomu wiersza poleceń urządzenia, na którym jest zainstalowany Serwer administracyjny.

Składnia wiersza poleceń narzędzia:

```
klbackup -path ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ [-logfile PLIKRAPORTU] [-use_ts]|[-restore] [-password HASŁO] [-online]
```

Jeśli w wierszu polecenia narzędzia klbackup nie określono hasła, narzędzie zażąda wprowadzenie hasła interaktywnie.

Opisy przełączników:

- `-path BACKUP_PATH`—zapisuje informacje w folderze ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ lub używa danych z folderu ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ do ich przywrócenia (wymagany parametr).

- `-logfile LOGFILE`—zapisuje raport dotyczący tworzenia kopii zapasowej i przywracania danych Serwera administracyjnego.

  Konto serwera bazy danych i narzędzie klbackup powinny mieć uprawnienia do zmiany danych w folderze ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ.

- `-use_ts` — Podczas zapisywania danych kopiuje informacje do folderu BACKUP_PATH, do podfolderu z nazwą zawierającą bieżącą datę systemową i czas działania w formacie `klbackup RRRR-MM-DD # GG-MM-SS`. Jeśli przełącznik nie został określony, informacje są zapisywane w głównym folderze ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ.

  Podczas próby zapisu informacji do folderu, w którym już znajduje się kopia zapasowa, zostaje wyświetlona wiadomość o błędzie. Żadne informacje nie zostaną zaktualizowane.

  Dostępność przełącznika `-use_ts` pozwala zachować archiwum danych Serwera administracyjnego. Na przykład jeśli klucz `-path` wskazuje folder `C:\KLBackups`, wówczas folder `klbackup 2022/6/19 # 11-30-18` przechowuje informacje o stanie Serwera administracyjnego na dzień 19 czerwca 2022 roku, godzina 11:30:18.

- `-restore`—przywraca dane Serwera administracyjnego. Przywracanie danych odbywa się w oparciu o informacje znajdujące się w folderze ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ. Jeśli żaden parametr nie jest dostępny, kopie zapasowe danych są tworzone w folderze ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ.

- `-password PASSWORD`—zapisuje lub przywraca certyfikat Serwera administracyjnego; aby zaszyfrować lub odszyfrować certyfikat, użyj hasła określonego przez parametr HASŁO.

  > Zapomnianego hasła nie można odzyskać. Nie ma wymagań dotyczących hasła. Długość hasła jest nieograniczona i możliwa jest również długość zerowa (brak hasła).

  Podczas przywracania danych powinieneś określić to samo hasło, które wprowadziłeś podczas tworzenia kopii zapasowej. Jeśli po utworzeniu kopii zapasowej ścieżka do folderu współdzielonego uległa zmianie, sprawdź działanie zadań wykorzystujących przywrócone dane (zadania przywracania i zadania zdalnej instalacji). Jeśli jest to konieczne, zmodyfikuj ustawienia tych zadań. Podczas przywracania danych z pliku kopii zapasowej nikt nie może mieć dostępu do folderu współdzielonego Serwera administracyjnego. Konto, z poziomu którego uruchamiane jest narzędzie klbackup, musi mieć pełen dostęp do folderu współdzielonego. Zalecamy uruchomienie narzędzia na nowo zainstalowanym Serwerze administracyjnym.

- `-online`—utwórz kopię zapasową danych Serwera administracyjnego, tworząc migawkę woluminu, aby zminimalizować czas offline Serwera administracyjnego. Jeśli używasz narzędzia do odzyskiwania danych, ta opcja jest ignorowana.

Przenoszenie Serwera administracyjnego na inne urządzenie

Jeśli chcesz użyć Serwera administracyjnego na nowym urządzeniu, możesz je przenieść w jeden z następujących sposobów:

- Przenieś Serwer administracyjny i serwer bazy danych na nowe urządzenie.

- Zachowaj serwer bazy danych na poprzednim urządzeniu i przenieś tylko Serwer administracyjny na nowe urządzenie.

W celu przeniesienia Serwera administracyjnego na nowe urządzenie:

1. Na poprzednim urządzeniu utwórz kopię zapasową danych Serwera administracyjnego.

   W tym celu możesz uruchomić zadanie tworzenia kopii zapasowej danych za pomocą Konsoli administracyjnej lub uruchomić narzędzie klbackup.

Jeśli używasz SQL Server jako DBMS dla Serwera administracyjnego, możesz migrować dane z SQL Server do MySQL lub MariaDB DBMS. Aby to zrobić, uruchom narzędzie klbackup w trybie interaktywnym, aby utworzyć kopię zapasową danych. Włącz opcję **Migracja do formatu MySQL/MariaDB** w oknie **Ustawienia kopii zapasowej** kopii zapasowej Kreatora kopii zapasowych i przywracania. Kaspersky Security Center utworzy kopię zapasową kompatybilną z MySQL i MariaDB. Następnie możesz przywrócić dane z kopii zapasowej do MySQL lub MariaDB.

Możesz również włączyć opcję **Wykonaj migrację do formatu Azure** jeśli chcesz migrować dane z SQL Server do Azure SQL DBMS.

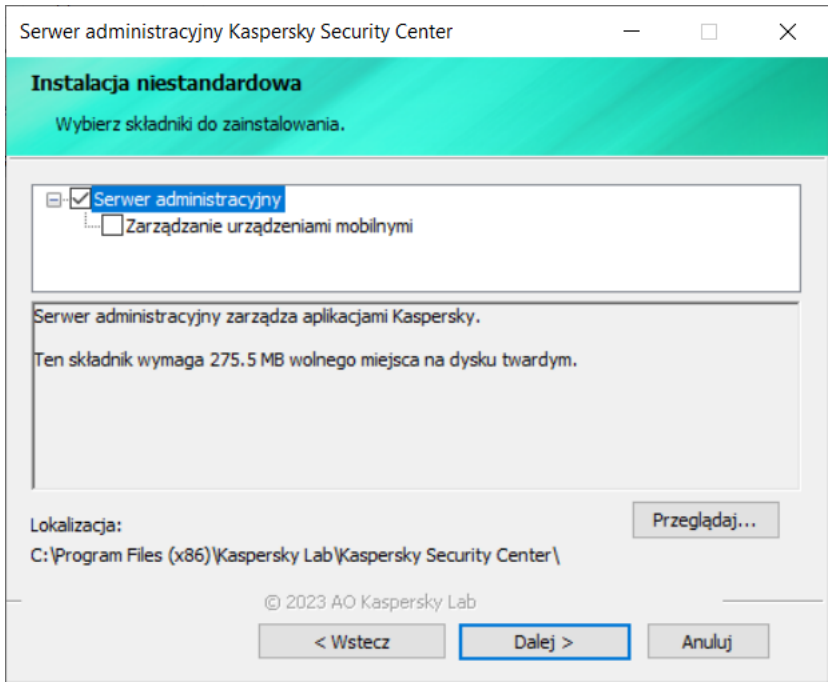
2. Wybierz nowe urządzenie, na którym chcesz zainstalować Serwer administracyjny. Upewnij się, że sprzęt i oprogramowanie na wybranym urządzeniu spełniają wymagania Serwera administracyjnego, Konsoli administracyjnej i Agenta sieciowego. Sprawdź również, czy dostępne są porty używane na Serwerze administracyjnym.

3. Na nowym urządzeniu zainstaluj system zarządzania bazą danych (DBMS), z którego będzie korzystał Serwer administracyjny.

   Kiedy wybierasz DBMS, weź pod uwagę liczbę urządzeń obsługiwanych przez Serwer administracyjny.

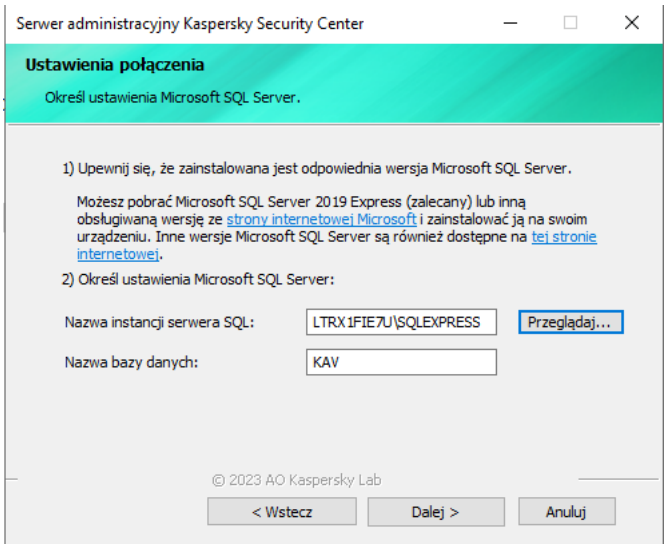
4. Uruchom niestandardową instalację Serwera administracyjnego na nowym urządzeniu.

5. Zainstaluj składniki Serwera administracyjnego w tym samym folderze, w którym Serwer administracyjny jest zainstalowany na poprzednim urządzeniu. Kliknij przycisk **Przeglądaj**, aby określić ścieżkę do pliku.



Okno instalacji niestandardowej

6. Skonfiguruj ustawienia połączenia z serwerem bazy danych.



Przykład okna Ustawienia połączenia dla Microsoft SQL Server

W zależności od tego, gdzie chcesz zlokalizować serwer bazy danych, wykonaj jedną z następujących czynności:

- Przenieś Serwer administracyjny na nowe urządzenie

  1. Kliknij przycisk **Przeglądaj** obok pola **Nazwa instancji serwera SQL**, a następnie wybierz nową nazwę urządzenia z wyświetlonej listy.
  2. Wprowadź nową nazwę bazy danych w polu **Nazwa bazy danych**.

     Należy pamiętać, że nazwa nowej bazy danych musi być zgodna z nazwą bazy danych z poprzedniego urządzenia. Nazwy baz danych muszą być identyczne, abyś mógł korzystać z kopii zapasowej Serwera administracyjnego. Domyślna nazwa bazy danych to *KAV*.

- Zachowaj serwer bazy danych na poprzednim urządzeniu

  1. Kliknij przycisk **Przeglądaj** obok pola **Nazwa instancji serwera SQL**, a następnie wybierz poprzednią nazwę urządzenia z wyświetlonej listy.

     Pamiętaj, że poprzednie urządzenie musi być dostępne do połączenia z nowym Serwerem administracyjnym.
  2. Wprowadź poprzednią nazwę bazy danych w polu **Nazwa bazy danych**.

7. Po zakończeniu instalacji odzyskaj dane Serwera administracyjnego na nowym urządzeniu za pomocą narzędzia klbackup.

   Jeśli używasz programu SQL Server jako DBMS na poprzednich i nowych urządzeniach, pamiętaj, że wersja programu SQL Server zainstalowana na nowym urządzeniu musi być taka sama lub nowsza niż wersja programu SQL Server zainstalowana na poprzednim urządzeniu. W przeciwnym razie nie będzie możliwe odzyskanie danych Serwera administracyjnego na nowym urządzeniu.

8. Otwórz Konsolę administracyjną do nawiązywania połączenia z Serwerem administracyjnym.

9. Sprawdź, czy wszystkie urządzenia klienckie są połączone z Serwerem administracyjnym.

10. Odinstaluj Serwer administracyjny i serwer bazy danych z poprzedniego urządzenia.

Możesz także użyć Kaspersky Security Center Web Console do przeniesienia Serwera administracyjnego i serwera bazy danych na inne urządzenie.

Unikanie konfliktów między kilkoma Serwerami administracyjnymi

Jeśli w sieci posiadasz więcej niż jeden Serwer administracyjny, mogą one widzieć te same urządzenia klienckie. Może to powodować, na przykład, zdalną instalację tej samej aplikacji na jednym i tym samym urządzeniu z więcej niż jednego Serwera oraz inne konflikty. Aby uniknąć takiej sytuacji, Kaspersky Security Center 14.2 pozwala zapobiegać instalacji aplikacji na urządzeniu zarządzanym przez inny Serwer administracyjny.

Możesz także użyć właściwości **Zarządzane przez inny Serwer administracyjny** jako kryterium dla:

- Wyszukiwania urządzeń
- Wybory urządzeń
- Reguły przenoszenia urządzeń
- Reguł automatycznego znakowania

Kaspersky Security Center 14.2 używa heurystyki do określenia, czy urządzenie klienckie jest zarządzane przez Serwer administracyjny, z którym pracujesz, lub przez inny Serwer administracyjny.

Weryfikacja dwuetapowa

Ta sekcja opisuje sposób korzystania z weryfikacji dwuetapowej do zmniejszenia ryzyka nieautoryzowanego dostępu do Konsoli administracyjnej lub Kaspersky Security Center Web Console.

Scenariusz: konfigurowanie weryfikacji dwuetapowej dla wszystkich użytkowników

W tym scenariuszu opisano sposób włączenia weryfikacji dwuetapowej dla wszystkich użytkowników oraz sposób wykluczenia konta użytkowników z weryfikacji dwuetapowej. Jeśli nie włączyłeś weryfikacji dwuetapowej dla swojego konta przed włączeniem go dla innych użytkowników, aplikacja najpierw otworzy okno umożliwiające włączenie weryfikacji dwuetapowej dla Twojego konta. W tym scenariuszu opisano również sposób włączenia weryfikacji dwuetapowej na swoim koncie.

Jeśli włączyłeś weryfikację dwuetapową na swoim koncie, możesz przejść do etapu włączenia weryfikacji dwuetapowej dla wszystkich użytkowników.

Wymagania wstępne

Zanim zaczniesz:

- Upewnij się, że Twoje konto użytkownika ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** służącym do modyfikacji ustawień zabezpieczeń dla kont innych użytkowników.
- Upewnij się, że inni użytkownicy Serwera administracyjnego zainstalowali aplikację uwierzytelniającą na swoich urządzeniach.

Etapy

Włączenie weryfikacji dwuetapowej dla wszystkich użytkowników przebiega etapami:

1. **Instalowanie aplikacji uwierzytelniającej na urządzeniu**

   Możesz zainstalować aplikację Google Authenticator, Microsoft Authenticator lub dowolną inną aplikację uwierzytelniającą, która obsługuje algorytm jednorazowego hasła czasowego.

2. **Synchronizacja czasu aplikacji uwierzytelniającej z czasem urządzenia, na którym zainstalowany jest Serwer administracyjny**

   Upewnij się, że czas ustawiony w aplikacji uwierzytelniającej jest zsynchronizowany z czasem Serwera administracyjnego.

3. **Włączenie weryfikacji dwuetapowej dla Twojego konta i otrzymanie tajnego klucza do Twojego konta**

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Włączanie weryfikacji dwuetapowej na własnym koncie
   - Dla Kaspersky Security Center Web Console: Włączanie weryfikacji dwuetapowej dla własnego konta

   Po włączeniu weryfikacji dwuetapowej na koncie możesz włączyć weryfikację dwuetapową dla wszystkich użytkowników.

4. **Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników**

   Użytkownicy z włączoną weryfikacją dwuetapową muszą jej używać do logowania się do Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników
   - Dla Kaspersky Security Center Web Console: Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników

5. **Edytowanie nazwy wystawcy kodu zabezpieczającego**

   Jeśli masz kilka Serwerów administracyjnych o podobnych nazwach, konieczna może być zmiana nazw wystawców kodów zabezpieczających w celu lepszego rozpoznawania różnych Serwerów administracyjnych.

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Edytowanie nazwy wystawcy kodu zabezpieczającego
   - Dla Kaspersky Security Center Web Console: Edytowanie nazwy wystawcy kodu zabezpieczającego

6. **Z wyłączeniem kont użytkowników, dla których nie musisz włączać weryfikacji dwuetapowej**

   W razie potrzeby możesz wykluczyć użytkowników z weryfikacji dwuetapowej. Użytkownicy z wykluczonymi kontami nie muszą używać weryfikacji dwuetapowej, aby zalogować się do Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna oparta na MMC: Wykluczanie kont z weryfikacji dwuetapowej
- Dla Kaspersky Security Center Web Console: Wykluczanie kont z weryfikacji dwuetapowej

Wyniki

Po zakończeniu tego scenariusza:

- Weryfikacja dwuetapowa jest włączona na Twoim koncie.
- Weryfikacja dwuetapowa jest włączona dla wszystkich kont użytkowników Serwera administracyjnego, z wyjątkiem kont użytkowników, które zostały wykluczone.

Informacje o weryfikacji dwuetapowej

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

Kod zabezpieczający posiada identyfikator, o którym mowa w *nazwie wystawcy*. Nazwa wystawcy kodu zabezpieczającego jest używana jako identyfikator Serwera administracyjnego w aplikacji uwierzytelniającej. Możesz zmienić nazwę wydawcy kodu zabezpieczającego. Nazwa wystawcy kodu zabezpieczającego ma domyślną wartość, która jest taka sama jak nazwa Serwera administracyjnego. Nazwa wystawcy jest używana jako identyfikator Serwera administracyjnego w aplikacji uwierzytelniającej. Jeśli zmienisz nazwę wystawcy kodu zabezpieczającego, musisz wydać nowy tajny klucz i przekazać go do aplikacji uwierzytelniającej. Kod zabezpieczający jest jednorazowy i ważny do 90 sekund (dokładny czas może się różnić).

Każdy użytkownik, dla którego włączono weryfikację dwuetapową, może ponownie wydać swój własny tajny klucz. Jeśli użytkownik uwierzytelnia się za pomocą ponownie wydanego tajnego klucza i używa go do logowania, Serwer administracyjny zapisuje nowy tajny klucz dla konta użytkownika. Jeśli użytkownik wprowadzi nowy tajny klucz niepoprawnie, Serwer administracyjny nie zapisze nowego tajnego klucza i pozostawi aktualny tajny klucz ważny do dalszej autoryzacji.

> Każde oprogramowanie uwierzytelniające, które obsługuje algorytm jednorazowego hasła czasowego (TOTP), może być używane jako aplikacja uwierzytelniająca, na przykład Google Authenticator. Aby wygenerować kod zabezpieczający, musisz zsynchronizować czas ustawiony w aplikacji uwierzytelniającej z czasem ustawionym dla Serwera administracyjnego.

Aplikacja uwierzytelniająca generuje kod zabezpieczający w następujący sposób:

1. Serwer administracyjny generuje specjalny tajny klucz i kod QR.
2. Przekazujesz wygenerowany tajny klucz lub kod QR do aplikacji uwierzytelniającej.
3. Aplikacja uwierzytelniająca generuje jednorazowy kod zabezpieczający, który należy przekazać do okna uwierzytelniania Serwera administracyjnego.

Zdecydowanie zalecamy zainstalowanie aplikacji uwierzytelniającej na więcej niż jednym urządzeniu. Zapisz tajny klucz (lub kod QR) i przechowuj go w bezpiecznym miejscu. Pomoże to w przywróceniu dostępu do Konsoli administracyjnej lub Kaspersky Security Center Web Console w przypadku utraty dostępu do urządzenia mobilnego.

Aby zabezpieczyć korzystanie z Kaspersky Security Center, możesz włączyć weryfikację dwuetapową dla swojego konta i włączyć weryfikację dwuetapową dla wszystkich użytkowników.

Możesz wykluczyć konta z weryfikacji dwuetapowej. Może to być konieczne w przypadku kont usług, które nie mogą otrzymać kodu zabezpieczającego dla uwierzytelnienia.

Weryfikacja dwuetapowa działa według następujących zasad:

- Tylko konto użytkownika z uprawnieniem Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** umożliwia weryfikację dwuetapową dla wszystkich użytkowników.
- Tylko użytkownik, który włączył weryfikację dwuetapową na swoim koncie, może włączyć opcję weryfikacji dwuetapowej dla wszystkich użytkowników.
- Tylko użytkownik, który włączył weryfikację dwuetapową na swoim koncie, może wykluczyć inne konta użytkowników z listy weryfikacji dwuetapowej włączonej dla wszystkich użytkowników.
- Użytkownik może włączyć weryfikację dwuetapową tylko dla swojego konta.
- Konto użytkownika, który posiada uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika** i jest zalogowany do Konsoli administracyjnej lub Kaspersky Security Center Web Console przy użyciu weryfikacji dwuetapowej, może wyłączyć weryfikację dwuetapową: dla każdego innego użytkownika tylko wtedy, gdy weryfikacja dwuetapowa dla wszystkich użytkowników jest wyłączona, dla użytkownika wykluczonego z listy weryfikacji dwuetapowej, która jest włączona dla wszystkich użytkowników.
- Każdy użytkownik, który zalogował się do Konsoli administracyjnej lub Kaspersky Security Center Web Console przy użyciu weryfikacji dwuetapowej, może ponownie wydać swój własny tajny klucz.
- Możesz włączyć opcję weryfikacji dwuetapowej dla wszystkich użytkowników dla Serwera administracyjnego, z którym aktualnie pracujesz. Jeśli włączysz tę opcję na Serwerze administracyjnym, włączysz tę opcję również dla jego kont użytkowników jego wirtualnych Serwerów administracyjnych i nie włączysz weryfikacji dwuetapowej dla kont użytkowników podrzędnych Serwerów administracyjnych.

Jeśli dla konta użytkownika na Serwerze administracyjnym Kaspersky Security Center 13 włączona jest weryfikacja dwuetapowa, użytkownik nie będzie mógł zalogować się do konsoli Kaspersky Security Center Web Console w wersji 12, 12.1 lub 12.2.

Włączanie weryfikacji dwuetapowej dla własnego konta

Zanim włączysz weryfikację dwuetapową na swoim koncie, upewnij się, że aplikacja uwierzytelniająca jest zainstalowana na Twoim urządzeniu mobilnym. Upewnij się, że czas ustawiony w aplikacji uwierzytelniającej jest zsynchronizowany z czasem Serwera administracyjnego.

W celu włączenia weryfikacji dwuetapowej na swoim koncie:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.

2. W oknie właściwości Serwera administracyjnego przejdź do panelu **Sekcje** i wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.

3. W sekcji **Weryfikacja dwuetapowa** kliknij przycisk **Konfiguruj**.

   W otwartym oknie właściwości weryfikacji dwuetapowej wyświetlany jest tajny klucz.

4. Wprowadź tajny klucz w aplikacji uwierzytelniającej, aby uzyskać jednorazowy kod zabezpieczający. Możesz podać tajny klucz w aplikacji uwierzytelniającej ręcznie lub zeskanować kod QR za pomocą urządzenia mobilnego.

5. Określ kod zabezpieczający wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **OK**, aby zamknąć okno właściwości weryfikacji dwuetapowej.

6. Kliknij przycisk **Zastosuj**.

7. Kliknij przycisk **OK**.

Weryfikacja dwuetapowa jest włączona na Twoim koncie.

Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników

Możesz włączyć weryfikację dwuetapową dla wszystkich użytkowników Serwera administracyjnego, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** i jeśli jesteś uwierzytelniony za pomocą weryfikacji dwuetapowej. Jeśli nie włączyłeś weryfikacji dwuetapowej na swoim koncie przed włączeniem jej dla wszystkich użytkowników, aplikacja otworzy okno dla włączenia weryfikacji dwuetapowej dla własnego konta.

W celu włączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.

2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.

3. Kliknij przycisk **Skonfiguruj wymagane**, aby włączyć weryfikację dwuetapową dla wszystkich użytkowników.

4. W sekcji **Weryfikacja dwuetapowa** kliknij przycisk **Zastosuj**, a następnie kliknij przycisk **OK**.

Weryfikacja dwuetapowa jest włączona dla wszystkich użytkowników. Od teraz wszyscy użytkownicy Serwera administracyjnego, w tym użytkownicy dodani po włączeniu tej opcji, muszą konfigurować weryfikację dwuetapową dla swoich kont, z wyjątkiem użytkowników, których konta są wykluczone z weryfikacji dwuetapowej.

Wyłączanie weryfikacji dwuetapowej dla konta użytkownika

W celu wyłączenia weryfikacji dwuetapowej na swoim koncie:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.
3. W sekcji **Weryfikacja dwuetapowa** kliknij przycisk **Wyłącz**.
4. Kliknij przycisk **Zastosuj**.
5. Kliknij przycisk **OK**.

Weryfikacja dwuetapowa jest wyłączona na Twoim koncie.

Możesz wyłączyć weryfikację dwuetapową kont innych użytkowników. Zapewnia to ochronę w przypadku, gdy, na przykład, użytkownik zgubi lub zepsuje urządzenie mobilne.

Możesz wyłączyć weryfikację dwuetapową konta innego użytkownika tylko wtedy, gdy masz uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika**. Wykonując poniższe czynności, możesz również wyłączyć weryfikację dwuetapową na swoim koncie.

W celu wyłączenia weryfikacji dwuetapowej dla dowolnego konta użytkownika:

1. W drzewie konsoli otwórz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.
2. W obszarze roboczym kliknij dwukrotnie konto użytkownika, dla którego chcesz wyłączyć weryfikację dwuetapową.
3. W oknie **Właściwości:<nazwa użytkownika>**, które zostanie otwarte, wybierz sekcję **Weryfikacja dwuetapowa**.
4. W sekcji **Weryfikacja dwuetapowa** wybierz następujące opcje:
   - Jeśli chcesz wyłączyć weryfikację dwuetapową dla konta użytkownika, kliknij przycisk **Wyłącz**.
   - Jeśli chcesz wykluczyć to konto użytkownika z weryfikacji dwuetapowej, wybierz opcję **Użytkownik może przejść uwierzytelnianie tylko przy użyciu nazwy użytkownika i hasła**.
5. Kliknij przycisk **Zastosuj**.
6. Kliknij przycisk **OK**.

Weryfikacja dwuetapowa dla konta użytkownika jest wyłączona.

Wyłączanie weryfikacji dwuetapowej dla wszystkich użytkowników

Możesz wyłączyć weryfikację dwuetapową dla wszystkich użytkowników Serwera administracyjnego, jeśli masz uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** i jeśli jesteś uwierzytelniony za pomocą weryfikacji dwuetapowej.

W celu wyłączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.
3. Kliknij przycisk **Skonfiguruj opcjonalne**, aby wyłączyć weryfikację dwuetapową dla wszystkich użytkowników.
4. Kliknij przycisk **Zastosuj** w sekcji **Weryfikacja dwuetapowa**.
5. Kliknij przycisk **OK** w sekcji **Weryfikacja dwuetapowa**.

Weryfikacja dwuetapowa jest wyłączona dla wszystkich użytkowników.

Wykluczanie kont z weryfikacji dwuetapowej

Możesz wykluczyć konto z weryfikacji dwuetapowej, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika**.

Jeśli konto użytkownika zostało wykluczone z weryfikacji dwuetapowej, użytkownik ten może zalogować się do Konsoli administracyjnej lub Kaspersky Security Center Web Console bez korzystania z weryfikacji dwuetapowej.

Wykluczenie kont z weryfikacji dwuetapowej może być konieczne w przypadku kont usług, które nie mogą przekazać kodu zabezpieczającego podczas uwierzytelniania.

W celu wykluczenia konta użytkownika z weryfikacji dwuetapowej:

1. Jeśli chcesz wykluczyć konto Active Directory, wykonaj Przeszukiwanie Active Directory, aby odświeżyć listę użytkowników Serwera administracyjnego.
2. W drzewie konsoli otwórz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.
3. W obszarze roboczym kliknij dwukrotnie konto użytkownika, które chcesz wykluczyć z weryfikacji dwuetapowej
4. W oknie **Właściwości:<nazwa użytkownika>**, które zostanie otwarte, wybierz sekcję **Weryfikacja dwuetapowa**.
5. W otwartej sekcji wybierz opcję **Użytkownik może przejść uwierzytelnianie tylko przy użyciu nazwy użytkownika i hasła**.
6. W sekcji **Weryfikacja dwuetapowa** kliknij przycisk **Zastosuj**, a następnie kliknij przycisk **OK**.

To konto użytkownika jest wykluczone z weryfikacji dwuetapowej. Wykluczone konta możesz sprawdzić na liście kont użytkowników.

Edytowanie nazwy wystawcy kodu zabezpieczającego

Możesz mieć kilka identyfikatorów (nazywanych wystawcami) dla różnych Serwerów administracyjnych. Możesz zmienić nazwę wystawcy kodu zabezpieczającego w przypadku, gdy, na przykład, Serwer administracyjny już używa podobnej nazwy wystawcy kodu zabezpieczającego dla innego Serwera administracyjnego. Domyślnie, nazwa wystawcy kodu zabezpieczającego jest taka sama, jak nazwa Serwera administracyjnego.

Po zmianie nazwy wystawcy kodu zabezpieczającego należy ponownie wystawić nowy tajny klucz i przekazać go do aplikacji uwierzytelniającej.

W celu określenia nowej nazwy wystawcy kodu zabezpieczającego:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **Zaawansowane**, a następnie **Weryfikacja dwuetapowa**.
3. Podaj nową nazwę wystawcy kodu zabezpieczającego w polu **Wystawca kodu zabezpieczającego**.
4. Kliknij przycisk **Zastosuj** w sekcji **Weryfikacja dwuetapowa**.
5. Kliknij przycisk **OK** w sekcji **Weryfikacja dwuetapowa**.

Nowa nazwa wystawcy kodu zabezpieczającego została określona dla Serwera administracyjnego.

Zmiana folderu współdzielonego Serwera administracyjnego

Folder współdzielony Serwera administracyjnego jest określany podczas instalacji Serwera administracyjnego. Zmiana lokalizacji folderu współdzielonego jest także możliwe we właściwościach Serwera administracyjnego.

Aby zmienić folder współdzielony:

1. Przypisz podgrupie **Wszyscy** prawa do pełnej kontroli do folderu, którego chcesz używać jako współdzielonego.
2. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w panelu Sekcje wybierz **Zaawansowane**, a następnie **Folder współdzielony Serwera administracyjnego**.
4. W sekcji **Folder współdzielony Serwera administracyjnego** kliknij przycisk **Zmień**.
5. Wybierz folder, którego chcesz użyć jako współdzielonego.
6. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.
7. Przypisz podgrupie **Wszyscy** prawa do odczytu do folderu, który został wybrany jako współdzielony.

Zarządzanie grupami administracyjnymi

Dostępne są tu informacje o sposobie zarządzania grupami administracyjnymi.

Na grupach administracyjnych możesz wykonać następujące akcje:

- Dodać do grup administracyjnych dowolną liczbę grup zagnieżdżonych z jakiegokolwiek poziomu hierarchii.
- Dodać urządzenia do grup administracyjnych.
- Zmienić hierarchię grup administracyjnych przez przeniesienie pojedynczych urządzeń i całych grup do innych grup.
- Usunąć grupy zagnieżdżone i urządzenia z grup administracyjnych.
- Dodać podrzędne i wirtualne Serwery administracyjne do grup administracyjnych.
- Przenieść urządzenia z grup administracyjnych Serwera administracyjnego do grup innego Serwera.
- Wskazać aplikacje Kaspersky, które będą automatycznie instalowane na urządzeniach znajdujących się w grupie.

Możesz wykonać te działania tylko wtedy, gdy posiadasz uprawnienie **Modyfikacja** w obszarze **Zarządzanie grupami administracyjnymi** dla grup administracyjnych, którymi chcesz zarządzać (lub dla Serwera administracyjnego, do którego te grupy należą).

Tworzenie grup administracyjnych

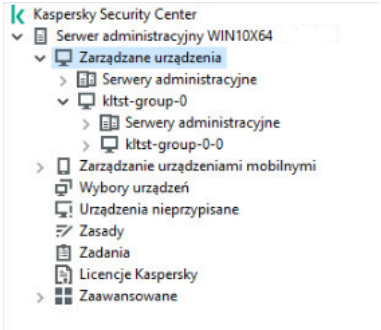
Hierarchia grup administracyjnych jest tworzona w oknie głównym aplikacji Kaspersky Security Center, w folderze **Zarządzane urządzenia**. Grupy administracyjne są wyświetlane w drzewie konsoli jako foldery (zobacz rysunek poniżej).

Natychmiast po zainstalowaniu Kaspersky Security Center, folder **Zarządzane urządzenia** będzie zawierał tylko pusty folder **Serwery administracyjne**.

> Ustawienia interfejsu użytkownika określają, czy folder **Serwery administracyjne** jest wyświetlany w drzewie konsoli. Aby wyświetlić ten folder, na pasku menu wybierz **Widok → Konfiguracja interfejsu** i w otwartym oknie **Konfiguracja interfejsu** zaznacz pole **Wyświetl podrzędne Serwery administracyjne**.

Podczas tworzenia hierarchii grup administracyjnych możesz dodać urządzenia i maszyny wirtualne do folderu **Zarządzane urządzenia**, a także możesz dodać zagnieżdżone grupy. Możesz dodać podrzędne i wirtualne Serwery administracyjne do folderu **Serwery administracyjne**.

Tak jak w folderze **Zarządzane urządzenia**, każda utworzona grupa początkowo zawiera tylko pusty folder **Serwery administracyjne**, który służy do pracy z podrzędnymi i wirtualnymi Serwerami administracyjnymi tej grupy. Informacje o zasadach i zadaniach dla tej grupy i jej urządzeniach wyświetlane są na zakładkach z odpowiednimi nazwami w obszarze roboczym tej grupy.



W celu utworzenia grupy administracyjnej:

1. W drzewie konsoli rozwiń folder **Zarządzane urządzenia**.
2. Jeśli chcesz utworzyć podgrupę w istniejącej grupie administracyjnej, w folderze **Zarządzane urządzenia** wybierz podfolder odpowiadający grupie, do której chcesz dodać nową grupę administracyjną.

   Jeśli tworzysz nową grupę administracyjną na najwyższym poziomie hierarchii, możesz pominąć ten krok.
3. Uruchom tworzenie grupy administracyjnej w jeden z następujących sposobów:
   - Korzystając z polecenia **Nowa** → **Grupa** z menu kontekstowego.
   - Klikając przycisk **Nowa grupa**, znajdujący się w obszarze roboczym okna głównego aplikacji, na zakładce **Urządzenia**.
4. W oknie **Nazwa grupy**, które zostanie otwarte, wprowadź nazwę grupy i kliknij **OK**.

W drzewie konsoli pojawi się nowy folder grupy administracyjnej o określonej nazwie.

Aplikacja umożliwia tworzenie hierarchii grup administracyjnych opartej na strukturze Active Directory lub na strukturze sieci domeny. Strukturę grup możesz również utworzyć z pliku tekstowego.

W celu utworzenia struktury grup administracyjnych:

1. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
2. Z menu kontekstowego folderu **Zarządzane urządzenia** wybierz **Wszystkie zadania** → **Nowa struktura grupy**.

Zostanie uruchomiony Kreator struktury nowej grupy administracyjnej. Postępuj zgodnie z instrukcjami kreatora.

Przenoszenie grup administracyjnych

Możliwe jest przenoszenie zagnieżdżonych grup administracyjnych w obrębie hierarchii grup.

Grupa administracyjna jest przenoszona wraz z grupami zagnieżdżonymi, podrzędnymi Serwerami administracyjnymi, urządzeniami, zasadami grupy i zadaniami. System zastosuje do grupy wszystkie ustawienia odpowiadające jej nowej pozycji w hierarchii grup administracyjnych.

Nazwa grupy musi być unikatowa w obrębie tego poziomu hierarchii. Jeżeli w folderze, do którego przenosisz grupę administracyjną, istnieje już grupa o takiej nazwie, powinieneś zmienić nazwę przenoszonej grupy. Jeżeli nie zmienisz nazwy przenoszonej grupy, do jej nazwy zostanie automatycznie dodany przyrostek **(<kolejny numer>)**, na przykład: **(1)**, **(2)**.

Nie można zmienić nazwy grupy **Zarządzane urządzenia**, ponieważ jest on wbudowanym elementem Konsoli administracyjnej.

W celu przeniesienia grupy do innego folderu w drzewie konsoli:

1. Wybierz grupę, którą chcesz przenieść.
2. Wykonaj jedną z poniższych czynności:

- Przenieś grupę, korzystając z menu kontekstowego:

  1. Wybierz **Wytnij** z menu kontekstowego grupy.

  2. Wybierz **Wklej** z menu kontekstowego grupy administracyjnej, do której chcesz przenieść wybraną grupę.

- Przenieś grupę, korzystając z menu okna głównego:

  a. Z głównego menu wybierz **Akcja** → **Wytnij**.

  b. Wybierz z drzewa konsoli grupę administracyjną, do której chcesz przenieść wybraną grupę.

  c. Z głównego menu wybierz **Akcja** → **Wklej**.

- Przenieść grupę do innej w drzewie konsoli, używając myszy.

Usuwanie grup administracyjnych

Możesz usunąć grupę administracyjną, jeżeli nie zawiera ona podrzędnych Serwerów administracyjnych, grup zagnieżdżonych lub urządzeń klienckich oraz gdy nie utworzono dla niej zasad lub zadań grupowych.

Przed usunięciem grupy administracyjnej należy usunąć z tej grupy wszystkie podrzędne Serwery administracyjne, grupy zagnieżdżone i urządzenia klienckie.

W celu usunięcia grupy:

1. Z drzewa konsoli wybierz grupę administracyjną.

2. Wykonaj jedną z poniższych czynności:

   - Wybierz **Usuń** z menu kontekstowego grupy.

   - Z głównego menu aplikacji wybierz **Akcja** → **Usuń**.

   - Wciśnij klawisz **DELETE**.

Automatyczne tworzenie struktury grup administracyjnych

Kaspersky Security Center umożliwia tworzenie struktury grup administracyjnych przy użyciu kreatora tworzenia hierarchii grup.

Kreator tworzy strukturę grup administracyjnych w oparciu o następujące dane:

- Struktury grup roboczych i domen Windows

- Struktury grup Active Directory

- Zawartość pliku tekstowego utworzonego ręcznie przez administratora

Podczas tworzenia pliku tekstowego muszą być spełnione następujące wymagania:

- Nazwa każdej nowej grupy musi znajdować się w nowej linii, a separator musi rozpoczynać się pustą linią. Puste linie są ignorowane.

  Na przykład:

  Office 1

  Office 2

  Office 3

  W grupie docelowej zostaną utworzone trzy grupy pierwszego poziomu hierarchii.

- Nazwę grupy zagnieżdżonej należy poprzedzić ukośnikiem (/).

  Na przykład:

  Office 1/Division 1/Department 1/Group 1

  W grupie docelowej zostaną utworzone cztery podgrupy zagnieżdżone w sobie.

- Aby utworzyć kilka grup zagnieżdżonych na tym samym poziomie hierarchii, należy określić "pełną ścieżkę do grupy".

  Na przykład:

  Office 1/Division 1/Department 1

  Office 1/Division 2/Department 1

  Office 1/Division 3/Department 1

  Office 1/Division 4/Department 1

  Jedna grupa pierwszego poziomu hierarchii Office 1 zostanie utworzona w grupie docelowej; grupa ta będzie zawierać cztery grupy zagnieżdżone tego samego poziomu hierarchii: "Division 1", "Division 2", "Division 3" i "Division 4". Każda z tych grup będzie zawierać grupę "Department 1".

Utworzenie hierarchii grup administracyjnych poprzez kreator nie ma wpływu na integralność sieci: zamiast zastępowania istniejących grup, dodawane są nowe grupy. Urządzenie klienckie nie może zostać przydzielone do grupy administracyjnej drugi raz, ponieważ urządzenie jest usuwane z grupy **Urządzenia nieprzypisane** po przeniesieniu go do grupy administracyjnej.

Jeśli podczas tworzenia struktury grupy administracyjnej urządzenie nie zostało umieszczone w grupie **Urządzenia nieprzypisane** (zostało zamknięte lub odłączone od sieci), nie zostanie automatycznie przeniesione do grupy administracyjnej. Urządzenia można dodać do grup administracyjnych ręcznie po zakończeniu działania kreatora.

W celu uruchomienia automatycznego tworzenia struktury grup administracyjnych:

1. W drzewie konsoli kliknij folder **Zarządzane urządzenia**.
2. Z menu kontekstowego folderu **Zarządzane urządzenia** wybierz **Wszystkie zadania → Nowa struktura grupy**.

Zostanie uruchomiony Kreator struktury nowej grupy administracyjnej. Postępuj zgodnie z instrukcjami kreatora.

Automatyczna instalacja aplikacji na urządzeniach w grupie administracyjnej

Możesz określić, które pakiety instalacyjne mają być użyte do automatycznej zdalnej instalacji aplikacji Kaspersky na urządzeniach klienckich, które zostały ostatnio dodane do grupy.

W celu skonfigurowania automatycznej instalacji aplikacji na nowych urządzeniach w grupie administracyjnej:

1. W drzewie konsoli wybierz żądaną grupę administracyjną.
2. Otwórz okno właściwości tej grupy administracyjnej.
3. W panelu **Sekcje** wybierz **Automatyczna instalacja**, a w obszarze roboczym wybierz pakiety instalacyjne aplikacji, które mają zostać zainstalowane na nowych urządzeniach.
4. Kliknij **OK**.

Zadania grupowe zostaną utworzone. Te zadania są uruchamiane na urządzeniach klienckich natychmiast po dodaniu ich do grupy administracyjnej.

W przypadku, gdy do automatycznej instalacji wybrano tylko niektóre pakiety instalacyjne danej aplikacji, zadanie instalacji zostanie utworzone tylko dla najnowszej wersji aplikacji.

Zarządzanie urządzeniami klienckimi

Ta sekcja zawiera informacje na temat pracy z urządzeniami klienckimi.

Łączenie urządzenia klienckiego z Serwerem administracyjnym

Połączenie między urządzeniem klienckim a Serwerem administracyjnym jest nawiązywane poprzez Agenta sieciowego zainstalowanego na urządzeniu klienckim.

Po połączeniu urządzenia klienckiego z Serwerem administracyjnym wykonywane są następujące działania:

- Automatyczna synchronizacja danych:
  - Synchronizacja listy aplikacji zainstalowanych na urządzeniu klienckim.
  - Synchronizacja profili, ustawień aplikacji, zadań oraz ustawień zadań.
- Odebranie aktualnych informacji o stanie aplikacji, wykonywaniu zadań i statystyk działania aplikacji przez Serwer administracyjny.
- Dostarczenie informacji o zdarzeniach na Serwer administracyjny w celu ich przetworzenia.

Automatyczna synchronizacja danych przeprowadzana jest regularnie zgodnie z ustawieniami Agenta sieciowego (przykładowo co piętnaście minut). Możesz określić ten czas ręcznie.

Informacja o zdarzeniu jest dostarczana do Serwera administracyjnego natychmiast po jego wystąpieniu.

Jeżeli Serwer administracyjny jest zdalny (znajduje się poza siecią firmową), urządzenia klienckie mogą łączyć się z nim przez internet.

Aby urządzenia klienckie łączyły się z Serwerem administracyjnym przez Internet, muszą być spełnione następujące warunki:

- Zdalny Serwer administracyjny musi posiadać zewnętrzny adres IP, a port dla ruchu przychodzącego o numerze 13000 musi pozostać otwarty (dla połączenia z Agentami sieciowymi). Zalecane jest także otwarcie portu UDP o numerze 13000 (do odbierania powiadomień o zamknięciu urządzeń).

- Agenty sieciowe powinny zostać zainstalowane na urządzeniach.

- Podczas instalacji Agenta sieciowego na urządzeniach powinieneś określić zewnętrzny adres IP zdalnego Serwera administracyjnego. Jeżeli do instalacji wykorzystywany jest pakiet instalacyjny, zewnętrzny adres IP jest określany ręcznie we właściwościach tego pakietu instalacyjnego, na zakładce **Ustawienia**.

- Aby użyć zdalnego Serwera administracyjnego do zarządzania aplikacjami i zadaniami dla urządzenia, w oknie właściwości tego urządzenia, w sekcji **Ogólny** zaznacz pole **Nie odłączaj od Serwera administracyjnego**. Po zaznaczeniu tego pola, należy zaczekać, aż Serwer administracyjny zsynchronizuje się ze zdalnym urządzeniem. Liczba urządzeń klienckich mających stałe połączenie z Serwerem administracyjnym nie może przekraczać 300.

Aby zwiększyć wydajność zadań zainicjowanych przez zdalny Serwer administracyjny, możesz otworzyć na urządzeniu port o numerze 15000. W tym przypadku, aby uruchomić zadanie, Serwer administracyjny wysyła specjalny pakiet do Agenta sieciowego przez port 15000, bez oczekiwania na zakończenie synchronizacji z urządzeniem.

Kaspersky Security Center pozwala na takie skonfigurowanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym, dzięki któremu połączenie pozostanie aktywne po zakończeniu wszystkich operacji. Stałe połączenie jest wymagane w przypadkach, gdy konieczne jest monitorowanie stanu aplikacji w czasie rzeczywistym, a Serwer administracyjny nie może połączyć się z klientem z jakiegoś powodu (na przykład, połączenie jest chronione przez zaporę sieciową, otwieranie portów na urządzeniu klienckim nie jest dozwolone lub adres IP urządzenia klienckiego nie jest znany). Stałe połączenie między urządzeniem klienckim a Serwerem administracyjnym można nawiązać w oknie właściwości urządzenia, w sekcji **Ogólny**.

Stałe połączenie zalecamy nawiązywać z najważniejszymi urządzeniami. Całkowita liczba jednocześnie utrzymywanych połączeń przez Serwer administracyjny jest ograniczona do 300.

Przy ręcznej synchronizacji system korzysta z pomocniczej metody łączenia, gdzie połączenie jest inicjowane przez Serwer administracyjny. Przed nawiązaniem połączenia na urządzeniu klienckim należy otworzyć port UDP. Serwer administracyjny wysyła żądanie połączenia na port UDP urządzenia klienckiego. W odpowiedzi weryfikowany jest certyfikat Serwera administracyjnego. Jeśli certyfikat Serwera administracyjnego odpowiada kopii certyfikatu przechowywanej na urządzeniu klienckim, rozpoczynane jest nawiązywanie połączenia.

Ręczne uruchamianie synchronizacji jest również wykorzystywane do uzyskiwania aktualnych informacji o stanie aplikacji, wykonywaniu zadań i statystyk działania aplikacji.

Ręczne łączenie urządzenia klienckiego z Serwerem administracyjnym. Narzędzie klmover

Jeżeli chcesz ręcznie połączyć urządzenie klienckie z Serwerem administracyjnym, możesz użyć na urządzeniu klienckim narzędzia klmover.

Podczas instalacji Agenta sieciowego na urządzeniach klienckich narzędzie jest automatycznie kopiowane do folderu instalacyjnego Agenta sieciowego.

W celu ręcznego połączenia urządzenia klienckiego z Serwerem administracyjnym, korzystając z narzędzia klmover:

Na urządzeniu uruchom narzędzie klmover z poziomu wiersza poleceń.

Po uruchomieniu narzędzia klmover z poziomu wiersza poleceń, będzie ono mogło wykonać następujące akcje (w zależności od używanych parametrów):

- Nawiązać połączenie między Agentem sieciowym a Serwerem administracyjnym, używając określonych ustawień;
- Zapisać wyniki działania w dzienniku zdarzeń lub wyświetlić je na ekranie.

Składnia wiersza poleceń narzędzia:

```
klmover [-logfile <file name>] [-address <server address>] [-pn <port number>] [-ps
<SSL port number>] [-nossl] [-cert <ścieżka do pliku certyfikatu>] [-silent] [-dupfix]
[-virtserv] [-cloningmode]
```

Do uruchomienia narzędzia wymagane są uprawnienia administratora.

Opisy przełączników:

- `-logfile <nazwa pliku>`—zapisuje wyniki działania narzędzia do pliku raportu.

  Domyślnie informacje są zapisywane w standardowym strumieniu wyjścia (stdout). Jeżeli parametr ten nie zostanie użyty, na ekranie zostaną wyświetlane wiadomości: o błędzie oraz z wynikami.

- `-address <adres serwera>`—adres Serwera administracyjnego, z którym nawiązywane jest połączenie.

  Jako adres można określić adres IP, nazwę NetBIOS lub nazwę DNS urządzenia.

- `-pn <numer portu>`—numer portu użytego do nawiązania nieszyfrowanego połączenia z Serwerem administracyjnym.

  Domyślny numer portu to 14000.

- `-ps <numer portu SSL>`—numer portu SSL, przez który nawiązywane jest połączenie szyfrowane z Serwerem administracyjnym (przy użyciu protokołu SSL).

  Domyślny numer portu to 13000.

- `-nossl`—użycie nieszyfrowanego połączenia z Serwerem administracyjnym.

  Jeżeli parametr ten nie zostanie użyty, Agent sieciowy nawiąże z Serwerem administracyjnym połączenie szyfrowane przy użyciu protokołu SSL.

- `-cert <ścieżka dostępu do pliku certyfikatu>`—użycie określonego pliku certyfikatu do autoryzacji podczas uzyskiwania dostępu do Serwera administracyjnego.

  Jeżeli parametr ten nie zostanie użyty, Agent sieciowy pobierze certyfikat podczas pierwszego połączenia z Serwerem administracyjnym.

- `-silent`—uruchamia narzędzie w trybie niezauważalnym dla użytkownika.

  Użycie tego parametru może być przydatne, gdy, na przykład, narzędzie jest uruchamiane ze skryptu logowania podczas rejestracji użytkownika.

- `-dupfix`—ten parametr jest używany, gdy Agent sieciowy został zainstalowany w sposób inny niż tradycyjny (z pakietu dystrybucyjnego), na przykład poprzez przywrócenie go z obrazu dysku ISO.

- `-virtserv`— Nazwa wirtualnego Serwera administracyjnego.

- `-cloningmode` — tryb klonowania dysku Agenta sieciowego.

  Użyj jednego z następujących parametrów, aby skonfigurować tryb klonowania dysku:

  - `-cloningmode` — Zażądaj stanu trybu klonowania dysku.
  - `-cloningmode 1` — Włącz tryb klonowania dysku.
  - `-cloningmode 0` — Wyłącz tryb klonowania dysku.

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

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

Tunelowanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym

Kaspersky Security Center umożliwia tunelowanie połączeń TCP z Konsoli administracyjnej poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym urządzeniu. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na urządzeniu z zainstalowaną Konsolą administracyjną z portem TCP na zarządzanym urządzeniu—jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a urządzeniem docelowym.

Na przykład, tunelowanie jest wykorzystywane dla połączeń ze zdalnym pulpitem - zarówno do łączenia się z istniejącą sesją, jak i do tworzenia nowej zdalnej sesji.

Tunelowanie połączeń może zostać włączone także przy użyciu narzędzi zewnętrznych. Na przykład, administrator może uruchomić w ten sposób narzędzie putty, klienta VNC oraz inne narzędzia.

Tunelowanie połączenia pomiędzy zdalnym urządzeniem klienckim a Serwerem administracyjnym jest wymagane, gdy port używany do nawiązania połączenia z Serwerem administracyjnym nie jest dostępny na urządzeniu. Port może być niedostępny na urządzeniu w następujących przypadkach:

- Zdalne urządzenie jest podłączone do sieci lokalnej, która wykorzystuje mechanizm NAT.
- Zdalne urządzenie jest częścią sieci lokalnej Serwera administracyjnego, ale jego port jest zamknięty przez zaporę sieciową.

W celu tunelowania połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym:

1. W drzewie konsoli wybierz folder grupy, która zawiera urządzenie klienckie.
2. Na zakładce **Urządzenia** wybierz urządzenie.
3. Z menu kontekstowego urządzenia wybierz **Wszystkie zadania → Tunelowanie połączenia**.
4. W otwartym oknie **Tunelowanie połączenia** utwórz tunel.

Zdalne połączenie z pulpitem urządzenia klienckiego

Administrator może uzyskać zdalny dostęp do pulpitu urządzenia klienckiego poprzez Agenta sieciowego zainstalowanego na urządzeniu klienckim.

Zdalne połączenie z urządzeniem poprzez Agenta sieciowego jest możliwe nawet wtedy, gdy porty TCP i UDP urządzenia klienckiego są zamknięte. Po nawiązaniu połączenia z urządzeniem, administrator uzyskuje pełny dostęp do informacji przechowywanych na tym urządzeniu, dzięki czemu może zarządzać aplikacjami, które są na nim zainstalowane.

W tej sekcji opisano sposób nawiązywania połączenia z urządzeniem klienckim Windows i urządzeniem klienckim macOS za pośrednictwem Agenta sieciowego.

Łączenie z urządzeniami klienckimi Windows

Zdalne połączenie z urządzeniem klienckim Windows można nawiązać w jeden z następujących sposobów:

- Używając standardowego składnika systemu Microsoft Windows o nazwie Podłączanie pulpitu zdalnego.

  Połączenie ze zdalnym pulpitem jest nawiązywane przy użyciu standardowego narzędzia Windows o nazwie mstsc.exe zgodnie z ustawieniami narzędzia.

- Używając technologii udostępniania pulpitu Windows.

Łączenie z urządzeniem klienckim z systemem Windows przy użyciu funkcji Podłączanie pulpitu zdalnego

Połączenie z bieżącą sesją zdalnego pulpitu użytkownika jest nawiązywane bez zgody użytkownika. Po nawiązaniu przez administratora połączenia z sesją, użytkownik urządzenia zostaje odłączony od sesji bez wcześniejszego powiadomienia.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego przy użyciu komponentu Podłączanie pulpitu zdalnego:

1. W drzewie Konsoli administracyjnej wybierz urządzenie, do którego chcesz uzyskać dostęp.
2. Z menu kontekstowego urządzenia wybierz **Wszystkie zadania → Połącz z urządzeniem → Nowa sesja Pulpitu zdalnego**.

   Zostanie uruchomione standardowe narzędzie systemu Windows o nazwie mstsc.exe, które pomoże w nawiązaniu połączenia ze zdalnym pulpitem.
3. Postępuj zgodnie z instrukcjami wyświetlanymi w oknach dialogowych narzędzia.

Po nawiązaniu połączenia z urządzeniem, pulpit jest dostępny w oknie Podłączanie pulpitu zdalnego systemu Microsoft Windows.

Łączenie z urządzeniem klienckim z systemem Windows przy użyciu funkcji Udostępnianie pulpitu w systemie Windows

Podczas łączenia się z istniejącą sesją zdalnego pulpitu użytkownik sesji na urządzeniu otrzymuje od administratora żądanie dotyczące połączenia. W raportach utworzonych przez Kaspersky Security Center nie są zapisywane żadne informacje dotyczące zdalnych działań wykonywanych na urządzeniu ani wyniki tych działań.

Administrator może połączyć się z istniejącą sesją na urządzeniu klienckim bez rozłączania użytkownika w tej sesji. W tym przypadku administrator i użytkownik sesji na urządzeniu klienckim współdzielą dostęp do pulpitu.

Administrator może skonfigurować audyt aktywności użytkownika na zdalnym urządzeniu klienckim. W trakcie audytu aplikacja zapisuje informacje o plikach na urządzeniu klienckim, który został otwarty i/lub zmodyfikowany przez administratora.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego poprzez udostępnianie pulpitu Windows muszą być spełnione następujące warunki:

- Na urządzeniu klienckim powinien być zainstalowany system operacyjny Microsoft Windows Vista lub nowszy system Windows.
- Na stacji roboczej administratora powinien być zainstalowany system operacyjny Microsoft Windows Vista lub nowszy. Typ systemu operacyjnego urządzenia, na którym znajduje się Serwer administracyjny nie nakłada żadnych ograniczeń na łączenie poprzez udostępnianie pulpitu Windows.

  Aby sprawdzić, czy funkcja udostępniania pulpitu Windows znajduje się w posiadanej przez Ciebie edycji systemu Windows, upewnij się, że klucz CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} znajduje się w rejestrze systemu Windows.
- System Microsoft Windows Vista lub nowszy jest zainstalowany na urządzeniu klienckim.
- Kaspersky Security Center korzysta z licencji dla Zarządzania lukami i poprawkami.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego poprzez udostępnianie pulpitu Windows:

1. W drzewie Konsoli administracyjnej wybierz urządzenie, do którego chcesz uzyskać dostęp.
2. Z menu kontekstowego urządzenia wybierz **Wszystkie zadania → Połącz z urządzeniem → Udostępnianie pulpitu Windows**.
3. W oknie **Wybierz sesję pulpitu zdalnego**, które zostanie otwarte, wybierz sesję na urządzeniu, do której chcesz się podłączyć.

   W przypadku pomyślnego nawiązania połączenia z urządzeniem, pulpit urządzenia będzie dostępny w oknie **Kaspersky Remote Desktop Session Viewer**.
4. Aby rozpocząć interakcję z urządzeniem, w menu głównym okna **Kaspersky Remote Desktop Session Viewer** wybierz **Akcje → Tryb interaktywny**.

Łączenie z urządzeniami klienckimi macOS

Administrator może używać systemu Virtual Network Computing (VNC) do łączenia się z urządzeniami macOS.

Połączenie ze zdalnym pulpitem jest nawiązywane za pośrednictwem klienta VNC zainstalowanego na urządzeniu Serwera administracyjnego. Klient VNC przełącza sterowanie klawiaturą i myszą z urządzenia klienckiego na administratora.

Gdy administrator łączy się ze zdalnym pulpitem, użytkownik nie otrzymuje powiadomień ani próśb o połączenie od administratora. Administrator łączy się z istniejącą sesją na urządzeniu klienckim bez rozłączania użytkownika w tej sesji.

W celu nawiązania połączenia z pulpitem macOS klienta poprzez klienta VNC muszą być spełnione następujące warunki:

- Klient VNC jest zainstalowany na urządzeniu Serwera administracyjnego.
- Zdalne logowanie i zdalne zarządzanie są dozwolone na urządzeniu klienckim.

- Użytkownik zezwolił administratorowi na dostęp do urządzenia klienckiego w ustawieniach **udostępniania** systemu operacyjnego macOS.

Aby połączyć się z pulpitem urządzenia klienckiego za pośrednictwem systemu Virtual Network Computing:

1. W drzewie Konsoli administracyjnej wybierz urządzenie, do którego chcesz uzyskać dostęp.
2. Z menu kontekstowego urządzenia wybierz **Wszystkie zadania → Tunelowanie połączenia**.
3. W otwartym oknie **Tunelowanie połączenia** wykonaj następujące czynności:
   a. W **1. Port sieciowy** określ numer portu sieciowego urządzenia, z którym chcesz się połączyć.
      Domyślnie wykorzystywany jest port 5900.
   b. W **2. Tunelowanie** kliknij przycisk **Utwórz tunel**.
   c. W **3. Ustawienia sieciowe** kliknij przycisk **Kopiuj**.
4. Otwórz klienta VNC i wklej skopiowane atrybuty sieciowe do pola tekstowego. Naciśnij **Enter**.
5. W oknie, które zostanie otwarte, przejrzyj szczegóły certyfikatu. Jeśli zgadzasz się na użycie certyfikatu, kliknij przycisk **Tak**.
6. W oknie **Uwierzytelnianie** określ poświadczenia urządzenia klienckiego, a następnie kliknij przycisk **OK**.

Nawiązywanie połączenia z urządzeniami poprzez udostępnianie pulpitu Windows

W celu nawiązania połączenia z urządzeniem poprzez udostępnianie pulpitu Windows:

1. W drzewie konsoli, na zakładce **Urządzenia** wybierz folder **Zarządzane urządzenia**.
   Obszar roboczy tego folderu wyświetla listę urządzeń.
2. Z menu kontekstowego urządzenia, z którym chcesz nawiązać połączenie, wybierz **Połącz z urządzeniem → Udostępnianie pulpitu Windows**.
   Zostanie otwarte okno **Wybierz sesję pulpitu zdalnego**.
3. W oknie **Wybierz sesję pulpitu zdalnego** wybierz sesję pulpitu w celu nawiązania połączenia z urządzeniem.
4. Kliknij **OK**.

Połączenie z urządzeniem zostanie nawiązane.

Konfigurowanie ponownego uruchamiania urządzenia klienckiego

Podczas korzystania, instalowania lub usuwania Kaspersky Security Center konieczne może być ponowne uruchomienie urządzenia. Możesz określić ustawienia ponownego uruchamiania tylko dla urządzeń działających pod kontrolą systemu Windows.

W celu skonfigurowania ponownego uruchamiania urządzenia klienckiego:

1. W drzewie konsoli należy wybrać grupę administracyjną, dla której chcesz skonfigurować ponowne uruchamianie.

2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.

3. W obszarze roboczym, na liście profili wybierz profil Agenta sieciowego Kaspersky Security Center, a następnie z menu kontekstowego profilu wybierz **Właściwości**.

4. W oknie ustawień zasady wybierz sekcję **Zarządzanie ponownym uruchamianiem**.

5. Wybierz akcję, jaka ma zostać wykonana, gdy wymagane jest ponowne uruchomienie urządzenia:

   - Wybierz **Nie uruchamiaj ponownie systemu operacyjnego**, aby zablokować automatyczne ponowne uruchamianie.

   - Wybierz **Jeżeli będzie to wymagane, automatycznie uruchom ponownie system operacyjny**, aby zezwolić na automatyczne ponowne uruchomienie.

   - Wybierz **Pytaj użytkownika o akcję**, aby włączyć wyświetlanie pytania o zezwolenie na ponowne uruchomienie.

   Można określić częstotliwość wyświetlania pytań o ponowne uruchomienie, włączyć wymuszone ponowne uruchomienie oraz wymuszone zamknięcie aplikacji w zablokowanych sesjach na urządzeniu, zaznaczając odpowiednie pola i ustawienia czasu w polu pokrętła.

6. Aby zapisać wprowadzone zmiany i zamknąć okno właściwości zasady, kliknij **OK**.

Ponowne uruchamianie urządzenia zostanie skonfigurowane.

Audyt działań na zdalnym urządzeniu klienckim

Aplikacja umożliwia przeprowadzenie audytu działań administratora na zdalnych urządzeniach klienckich działających pod kontrolą systemu Windows. W trakcie audytu aplikacja zapisuje na urządzeniu informacje o plikach, które zostały otwarte i/lub zmodyfikowane przez administratora. Audyt działań administratora jest dostępny, gdy są spełnione następujące warunki:

- Licencja Zarządzanie lukami i poprawkami jest w użyciu.

- Administrator posiada uprawnienie do włączania współdzielonego dostępu do pulpitu zdalnego urządzenia.

W celu włączenia audytu działań na zdalnym urządzeniu klienckim:

1. W drzewie konsoli wybierz grupę administracyjną, dla której powinien zostać skonfigurowany audyt działań administratora.

2. W obszarze roboczym grupy wybierz zakładkę **Zasady**.

3. Wybierz profil Agenta sieciowego Kaspersky Security Center, a następnie z menu kontekstowego zasady wybierz **Właściwości**.

4. W oknie ustawień zasady wybierz sekcję **Udostępnianie pulpitu Windows**.

5. Zaznacz pole **Włącz audyt**.

6. Na listach **Maski plików, które będą monitorowane podczas odczytu** i **Maski plików, które będą monitorowane podczas modyfikacji** dodaj maski plików, na których wykonywane działania mają być monitorowane przez aplikację podczas audytu.

   Domyślnie aplikacja monitoruje działania wykonywane na plikach z rozszerzeniami .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt i .pdf.

7. Aby zapisać wprowadzone zmiany i zamknąć okno właściwości zasady, kliknij **OK**.

Audyt działań administratora na zdalnym urządzeniu użytkownika z włączonym dostępem do pulpitu został skonfigurowany.

Wpisy dotyczące działań administratora na zdalnym urządzeniu są zapisywane w:

- Raporcie zdarzeń na zdalnym urządzeniu.
- Pliku z rozszerzeniem syslog znajdującym się w folderze Agenta sieciowego na zdalnym urządzeniu (na przykład: C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- Bazie danych zdarzeń programu Kaspersky Security Center.

Sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym

Kaspersky Security Center umożliwia ręczne lub automatyczne sprawdzanie połączeń między urządzeniem klienckim a Serwerem administracyjnym.

Automatyczne sprawdzanie połączeń odbywa się na Serwerze administracyjnym. Ręczne sprawdzanie połączeń wykonywane jest na urządzeniu.

Automatyczne sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym

W celu włączenia automatycznego sprawdzania połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym:

1. W drzewie konsoli wybierz grupę administracyjną, która zawiera urządzenia.
2. W obszarze roboczym grupy administracyjnej, na zakładce **Urządzenia** wybierz urządzenia.
3. Z otwartego menu kontekstowego urządzenia wybierz **Sprawdź dostępność urządzenia**.

Zostanie otwarte okno zawierające informacje o dostępności urządzenia.

Ręczne sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Narzędzie klnagchk

Możesz sprawdzić połączenie oraz uzyskać szczegółowe informacje o ustawieniach połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym, korzystając z narzędzia klnagchk.

Podczas instalacji Agenta sieciowego na urządzeniu narzędzie klnagchk jest automatycznie kopiowane do folderu instalacyjnego Agenta sieciowego.

Po uruchomieniu narzędzia klnagchk z poziomu wiersza poleceń będzie ono mogło wykonać następujące akcje (w zależności od używanych parametrów):

- Wyświetla na ekranie lub zapisuje w raporcie wartości ustawień używanych do łączenia Agenta sieciowego, zainstalowanego na urządzeniu, z Serwerem administracyjnym.
- Zapisać do pliku dziennika zdarzeń statystyki Agenta sieciowego (od jego ostatniego uruchomienia) oraz wyniki działania narzędzia lub wyświetlić informacje na ekranie.
- Podjąć próbę nawiązania połączenia pomiędzy Agentem sieciowym a Serwerem administracyjnym.

  Jeżeli próba nawiązania połączenia nie powiedzie się, narzędzie wyśle pakiet ICMP w celu sprawdzenia stanu urządzenia, na którym zainstalowany jest Serwer administracyjny.

W celu sprawdzenia połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym, korzystając z narzędzia klnagchk:

Na urządzeniu uruchom narzędzie klnagchk z poziomu wiersza poleceń.

Składnia wiersza poleceń narzędzia:

```
klnagchk [-logfile <nazwa pliku>] [-sp] [-savecert <ścieżka dostępu do pliku
certyfikatu>] [-restart]
```

Opisy przełączników:

- `-logfile <nazwa pliku>` —zapisuje do pliku raportu wartości ustawień połączenia pomiędzy Agentem sieciowym a Serwerem administracyjnym oraz wyniki działania narzędzia.

  Domyślnie informacje są zapisywane w standardowym strumieniu wyjścia (stdout). Jeżeli parametr ten nie zostanie użyty, na ekranie zostaną wyświetlane wiadomości: o błędzie, z wynikami oraz ustawieniami.
- `-sp` —wyświetla hasło używane do autoryzacji użytkownika na serwerze proxy.

  Ustawienie jest używane, jeśli połączenie z Serwerem administracyjnym jest nawiązywane za pośrednictwem serwera proxy.
- `-savecert <nazwa_pliku>` —zapisanie w określonym pliku certyfikatu używanego do uzyskiwania dostępu do Serwera administracyjnego.
- `-restart` —ponowne uruchomienie Agenta sieciowego po zakończeniu działania narzędzia.

Informacje o sprawdzaniu czasu połączenia pomiędzy urządzeniem a Serwerem administracyjnym

Po wyłączeniu urządzenia, Agent sieciowy powiadamia Serwer administracyjny o tym zdarzeniu. W Konsoli administracyjnej to urządzenie jest wyświetlane jako wyłączone. Jednakże Agent sieciowy nie może powiadamiać Serwera administracyjnego o wszystkich tego typu zdarzeniach. Dlatego też Serwer administracyjny okresowo analizuje atrybut **Połączono z Serwerem administracyjnym** (wartość tego atrybutu jest wyświetlana w Konsoli administracyjnej, we właściwościach urządzenia, w sekcji **Ogólny**) dla każdego urządzenia i porównuje go z interwałem synchronizacji z aktualnych ustawień Agenta sieciowego. Jeśli urządzenie nie odpowiedziało w ponad trzech pomyślnych interwałach synchronizacji, to urządzenie zostanie oznaczone jako wyłączone.

Identyfikowanie urządzeń klienckich na Serwerze administracyjnym

Urządzenia klienckie są identyfikowane w oparciu o ich nazwy. Nazwa urządzenia musi być unikatowa w obrębie wszystkich urządzeń połączonych z Serwerem administracyjnym.

Nazwa urządzenia jest przesyłana do Serwera administracyjnego podczas przeszukiwania sieci Windows i po wykryciu w niej nowego urządzenia lub przy pierwszym połączeniu Agenta sieciowego, zainstalowanego na urządzeniu, z Serwerem administracyjnym. Domyślnie nazwa odpowiada nazwie urządzenia w sieci Windows (nazwa NetBIOS). Jeśli na Serwerze administracyjnym jest już zarejestrowane urządzenie o tej nazwie, do nazwy nowego urządzenia zostanie dodany przyrostek z liczbą, na przykład: **<Nazwa>-1**, **<Nazwa>-2**. Pod tą nazwą urządzenie jest dodawane do grupy administracyjnej.

Przenoszenie urządzeń do grupy administracyjnej

Możesz przenosić urządzenia z jednej grupy administracyjnej do innej, jeśli posiadasz uprawnienie **Modyfikacja** w obszarze **Zarządzanie grupami administracyjnymi** dla źródłowej i docelowej grupy administracyjnej (lub dla Serwera administracyjnego, do którego te grupy należą).

W celu dodania jednego lub kilku urządzeń do wybranej grupy administracyjnej:

1. W drzewie konsoli rozwiń folder **Zarządzane urządzenia**.
2. W folderze **Zarządzane urządzenia** wybierz podfolder odpowiadający grupie, w której zostaną umieszczone urządzenia klienckie.

   Jeżeli chcesz dodać urządzenia do grupy **Zarządzane urządzenia**, możesz pominąć ten krok.
3. W obszarze roboczym wybranej grupy administracyjnej, na zakładce **Urządzenia** uruchom proces dodawania urządzeń do grupy w jeden z następujących sposobów:

   - Dodając urządzenia do grupy poprzez kliknięcie przycisku **Przenieś urządzenia do grupy** znajdującego się w oknie z informacjami dla listy urządzeń
   - Wybierając **Utwórz** → **Urządzenie** z menu kontekstowego listy urządzeń

   Zostanie uruchomiony Kreator przenoszenia urządzeń. Postępując zgodnie z jego poleceniami, wybierz metodę przenoszenia urządzeń do grupy i utwórz listę urządzeń, które mają zostać dodane do grupy.

   Jeżeli ręcznie tworzysz listę urządzeń, jako adres urządzenia możesz określić adres IP (lub zakres IP), nazwę NetBIOS lub nazwę DNS. Do listy możesz przenieść ręcznie tylko urządzenia, dla których informacje zostały już dodane do bazy danych Serwera administracyjnego przy podłączeniu urządzenia lub po wyszukiwaniu urządzeń.

   W celu zaimportowania listy urządzeń z pliku, należy wskazać plik TXT zawierający listę adresów urządzeń, które mają zostać dodane. Każdy adres musi znajdować się w oddzielnym wierszu.

Po zakończeniu pracy kreatora, wybrane urządzenia zostaną włączone do grupy administracyjnej i będą wyświetlane na liście urządzeń pod nazwami wygenerowanymi przez Serwer administracyjny.

Możesz przenieść urządzenie do wybranej grupy administracyjnej, przeciągając je z folderu **Urządzenia nieprzypisane** do folderu tej grupy administracyjnej.

Zmienianie Serwera administracyjnego dla urządzeń klienckich

Można zmienić Serwer administracyjny zarządzający urządzeniami klienckimi na inny, używając zadania *Zmiana Serwera administracyjnego*.

W celu zmiany Serwera administracyjnego zarządzającego urządzeniami klienckimi na inny Serwer:

1. Nawiąż połączenie z Serwerem administracyjnym, który zarządza urządzeniami.
2. Utwórz zadanie zmiany Serwera administracyjnego przy użyciu jednej z następujących metod:
   - Jeżeli chcesz zmienić Serwer administracyjny dla urządzeń znajdujących się w wybranej grupie administracyjnej, utwórz zadanie dla wybranej grupy.
   - Jeżeli chcesz zmienić Serwer administracyjny dla urządzeń znajdujących się w różnych grupach administracyjnych lub nie będących w żadnej istniejącej grupie administracyjnej, utwórz zadanie dla wskazanych urządzeń.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora. W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania wybierz węzeł **Kaspersky Security Center**, otwórz folder **Zaawansowane** i wybierz zadanie *Zmiana Serwera administracyjnego*.
3. Uruchom utworzone zadanie.

Po zakończeniu wykonywania zadania, urządzenia klienckie, dla których zostało ono utworzone, zostaną przekazane Serwerowi administracyjnemu określonemu w ustawieniach zadania.

Jeśli Serwer administracyjny obsługuje szyfrowanie i ochronę danych, a Ty tworzysz zadanie *Zmiana Serwera administracyjnego*, zostanie wyświetlone ostrzeżenie. Ostrzeżenie informuje, że jeśli jakiekolwiek zaszyfrowane dane są przechowywane na urządzeniach, po rozpoczęciu przez nowy Serwer zarządzania urządzeniami, użytkownicy będą mieli dostęp tylko do zaszyfrowanych danych, z którymi wcześniej pracowali. W innych przypadkach dostęp do zaszyfrowanych danych będzie niemożliwy. Szczegółowe opisy scenariuszy, w których dostęp do zaszyfrowanych danych nie jest zapewniany, znajdują się w Pomocy Kaspersky Endpoint Security for Windows.

Klastry i grupy serwerów

Kaspersky Security Center obsługuje technologię klastra. Jeśli Agent sieciowy wyśle na Serwer administracyjny informacje potwierdzające, że aplikacja zainstalowana na urządzeniu klienckim jest częścią grupy serwerów, to urządzenie klienckie staje się węzłem klastra. Klaster zostanie dodany jako odrębny obiekt w folderze **Zarządzane urządzenia** w drzewie konsoli z ikoną serwera ( ).

Możemy wyróżnić kilka typowych cech klastra:

- Klaster i każdy z jego węzłów są zawsze w tej samej grupie administracyjnej.
- Jeśli administrator spróbuje przenieść węzeł klastra, węzeł wróci do swojej oryginalnej lokalizacji.

- Jeśli administrator spróbuje przenieść klaster do innej grupy, wszystkie jego węzły zostaną przeniesione wraz z nim.

Zdalne włączanie, wyłączanie i ponowne uruchamianie urządzeń klienckich

Kaspersky Security Center pozwala na zdalne zarządzanie urządzeniami klienckimi: włączanie, wyłączanie i ponowne uruchamianie.

W celu zdalnego zarządzania urządzeniami klienckimi:

1. Nawiąż połączenie z Serwerem administracyjnym, który zarządza urządzeniami.
2. Utwórz zadanie zarządzania urządzeniami przy użyciu jednej z następujących metod:
   - Jeżeli chcesz włączyć, wyłączyć lub uruchomić ponownie urządzenia znajdujące się w wybranej grupie administracyjnej, utwórz zadanie dla wybranej grupy.
   - Jeżeli chcesz włączyć, wyłączyć lub uruchomić ponownie urządzenia znajdujące się w różnych grupach administracyjnych lub nie należące do żadnej z grup, utwórz zadanie dla wskazanych urządzeń.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora. W oknie **Wybierz typ zadania** kreatora tworzenia nowego zadania wybierz węzeł **Kaspersky Security Center**, otwórz folder **Zaawansowane** i wybierz zadanie **Zarządzaj urządzeniami**.
3. Uruchom utworzone zadanie.

   Po zakończeniu zadania, polecenie (włącz, wyłącz lub uruchom ponownie) zostanie wykonane na wybranych urządzeniach.

Informacje o korzystaniu z ciągłego połączenia pomiędzy zarządzanym urządzeniem a Serwerem administracyjnym

Domyślnie Kaspersky Security Center nie oferuje stałego połączenia pomiędzy zarządzanymi urządzeniami a Serwerem administracyjnym. Agenty sieciowe na zarządzanych urządzeniach okresowo nawiązują połączenie i synchronizują się z Serwerem administracyjnym. Odstęp pomiędzy tymi sesjami synchronizacji jest zdefiniowany w zasadzie Agenta sieciowego i domyślnie wynosi 15 minut. Jeśli wymagana jest wczesna synchronizacja (na przykład, aby wymusić zastosowanie zasady), Serwer administracyjny wysyła podpisany pakiet sieciowy do Agenta sieciowego na porcie UDP o numerze 15000 (Serwer administracyjny może wysłać ten pakiet poprzez sieć IPv4 lub IPv6). Jeśli z jakiegoś powodu nie jest możliwe nawiązanie połączenia poprzez UDP między Serwerem administracyjnym a zarządzanym urządzeniem, synchronizacja zostanie uruchomiona przy kolejnym rutynowym nawiązaniu połączenia między Agentem sieciowym a Serwerem administracyjnym w obrębie interwału synchronizacji.

Jednakże niektórych operacji nie można jednak wykonać bez wcześniejszego nawiązania połączenia między Agentem sieciowym a Serwerem administracyjnym. Operacje te obejmują uruchamianie i zatrzymywanie zadań lokalnych, odbieranie statystyk dla zarządzanej aplikacji i tworzenie tunelu. Aby te operacje były możliwe, musisz włączyć opcję **Nie odłączaj od Serwera administracyjnego** na zarządzanym urządzeniu.

Informacje o wymuszonej synchronizacji

Chociaż Kaspersky Security Center automatycznie synchronizuje stan, ustawienia, zadania i profile dla zarządzanych urządzeń, to w niektórych przypadkach administrator musi dokładnie wiedzieć, czy dla określonego urządzenia w danym momencie została już przeprowadzona synchronizacja.

W menu kontekstowym zarządzanych urządzeń w Konsoli administracyjnej urządzenia element menu **Wszystkie zadania** zawiera polecenie **Wymuś synchronizację**. Jeśli Kaspersky Security Center 14.2 wykona to polecenie, Serwer administracyjny podejmie próbę nawiązania połączenia z urządzeniem. Jeśli ta próba zakończy się pomyślnie, zostanie wykonana wymuszona synchronizacja. W innym przypadku synchronizacja zostanie wymuszona dopiero po kolejnym zaplanowanym połączeniu nawiązanym pomiędzy Agentem sieciowym a Serwerem administracyjnym.

Informacje o terminarzu połączenia

W oknie właściwości Agenta sieciowego, w sekcji **Łączność**, w podsekcji **Terminarz połączeń** możesz określić przedziały czasu, w trakcie których Agent sieciowy prześle dane do Serwera administracyjnego.

Połącz, gdy jest to konieczne. Jeśli ta opcja jest zaznaczona, połączenie jest nawiązywane, gdy Agent sieciowy musi wysłać dane na Serwer administracyjny.

Połącz w określonych przedziałach czasu. Jeśli ta opcja jest zaznaczona, Agent sieciowy łączy się z Serwerem administracyjnym w określonym czasie. Możesz dodać kilka przedziałów czasu.

Wysyłanie wiadomości na urządzenia użytkowników

W celu wysyłania wiadomości do użytkowników urządzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. Utwórz zadanie wysyłania wiadomości dla użytkowników urządzeń na jeden z następujących sposobów:
   - Jeśli chcesz wysłać wiadomość do użytkowników urządzeń należących do wybranej grupy administracyjnej, utwórz zadanie dla wybranej grupy.
   - Jeżeli chcesz wysłać wiadomość do użytkowników urządzeń należących do różnych grup administracyjnych lub nie będących w żadnej grupie administracyjnej, utwórz zadanie dla wskazanych urządzeń.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.
3. W oknie Typ zadania kreatora tworzenia nowego zadania wybierz węzeł **Serwer administracyjny Kaspersky Security Center**, otwórz folder **Zaawansowane** i wybierz zadanie **Wyślij wiadomość do użytkownika**. Zadanie wysyłania wiadomości do użytkownika jest dostępne tylko dla urządzeń działających pod kontrolą systemu Windows. Wiadomości możesz wysyłać także z poziomu menu kontekstowego w folderze **Konta użytkowników**.
4. Uruchom utworzone zadanie.

   Po zakończeniu wykonywania zadania utworzona wiadomość zostanie wysłana do użytkowników wybranych urządzeń. Zadanie wysyłania wiadomości do użytkownika jest dostępne tylko dla urządzeń działających pod kontrolą systemu Windows. Wiadomości możesz wysyłać także z poziomu menu kontekstowego w folderze **Konta użytkowników**.

Zarządzanie Kaspersky Security for Virtualization

Kaspersky Security Center obsługuje opcję łączenia maszyn wirtualnych z Serwerem administracyjnym. Maszyny wirtualne są chronione przez Kaspersky Security for Virtualization. Więcej informacji można znaleźć w dokumentacji dla tej aplikacji.

Konfigurowanie przełączania stanów urządzeń

Możesz zmienić warunki, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia.

W celu włączenia zmiany stanu urządzenia na Krytyczny:

1. Otwórz okno właściwości w jeden z następujących sposobów:
   - W folderze **Zasady**, w menu kontekstowym profilu Serwera administracyjnego wybierz **Właściwości**.
   - Z menu kontekstowego grupy administracyjnej wybierz **Właściwości**.
2. W oknie **Właściwości**, które zostanie otwarte, w panelu **Sekcje** wybierz **Stan urządzenia**.
3. W sekcji **Ustaw stan Krytyczny, jeśli** zaznacz pole obok warunku na liście.

   Jednakże możesz zmienić ustawienia, które nie są zablokowane w profilu nadrzędnym.

4. Dla wybranego warunku ustaw żądaną wartość.
   Możesz ustawić wartości dla niektórych, ale nie wszystkich, warunków.
5. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Krytyczne*.

W celu włączenia zmiany stanu urządzenia na Ostrzeżenie:

1. Otwórz okno właściwości w jeden z następujących sposobów:
   - W folderze **Zasady**, w menu kontekstowym profilu Serwera administracyjnego wybierz **Właściwości**.
   - Z menu kontekstowego grupy administracyjnej wybierz **Właściwości**.
2. W oknie **Właściwości**, które zostanie otwarte, w panelu **Sekcje** wybierz **Stan urządzenia**.
3. W prawej części, w sekcji **Ustaw stan Ostrzeżenie, jeśli** zaznacz pole obok warunku na liście.

   Jednakże możesz zmienić ustawienia, które nie są zablokowane w profilu nadrzędnym.

4. Dla wybranego warunku ustaw żądaną wartość.
   Możesz ustawić wartości dla niektórych, ale nie wszystkich, warunków.
5. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Ostrzeżenie*.

Znakowanie urządzeń i przeglądanie przydzielonych znaczników

Kaspersky Security Center umożliwia znakowanie urządzeń. *Znacznik* to identyfikator urządzenia, który może zostać użyty do grupowania, opisywania lub wyszukiwania urządzeń. Znaczniki przydzielone do urządzeń mogą być użyte do tworzenia wyborów, wyszukiwania urządzeń i rozdzielania urządzeń pomiędzy grupami administracyjnymi.

Urządzenia można znakować ręcznie lub automatycznie. Oznacz urządzenie ręcznie we właściwościach urządzenia; możesz skorzystać z ręcznego znakowania, jeśli musisz oznaczyć pojedyncze urządzenie. Automatyczne znakowanie jest wykonywane przez Serwer administracyjny zgodnie z określonymi regułami znakowania.

We właściwościach Serwera administracyjnego możesz skonfigurować automatyczne znakowanie dla urządzeń zarządzanych przez ten Serwer administracyjny. Urządzenia są znakowane automatycznie, gdy spełnione są określone reguły. Każdemu znacznikowi odpowiada pojedyncza reguła. Reguły są stosowane do właściwości sieciowych urządzenia, systemu operacyjnego, aplikacji zainstalowanych na urządzeniu i innych właściwości urządzenia. Na przykład, możesz skonfigurować regułę, która przypisze znacznik *Win* do wszystkich urządzeń działających pod kontrolą systemu Windows. Następnie możesz użyć tego znacznika podczas tworzenia wyboru urządzeń; pomoże to w sortowaniu wszystkich urządzeń z systemem Windows i przypisaniu do nich zadania.

Możesz także użyć znaczników jako warunków aktywacji profilu zasad na zarządzanym urządzeniu w celu zastosowania określonych profili zasad tylko na urządzeniach z określonymi znacznikami. Na przykład, jeśli urządzenie oznaczone jako *Kurier* pojawi się w grupie administracyjnej *Użytkownicy* i jeśli została włączona aktywacja odpowiedniego profilu zasad przez znacznik *Kurier*, wówczas profil utworzony dla grupy *Użytkownicy* nie zostanie zastosowany do tego urządzenia—ale profil profilu zasad zostanie zastosowany. Profil zasad może zezwolić temu urządzeniu na uruchamianie niektórych aplikacji, których uruchamianie zostało zablokowane przez profil.

Możesz utworzyć kilka reguł znakowania. Do jednego urządzenia może zostać przypisanych kilka znaczników, jeśli utworzyłeś kilka reguł znakowania i jeśli odpowiednie warunki tych reguł są spełnione w tym samym czasie. Listę wszystkich przydzielonych znaczników można przejrzeć we właściwościach urządzenia. Każda reguła znakowania może zostać włączona lub wyłączona. Jeśli reguła jest włączona, jest ona stosowana do urządzenia zarządzanego przez Serwer administracyjny. Jeśli aktualnie nie korzystasz z reguły, ale możesz potrzebować jej w przyszłości, nie musisz jej usuwać, możesz po prostu odznaczyć pole **Włącz regułę**. W tej sytuacji reguła zostanie wyłączona; nie będzie używana, aż do ponownego zaznaczenia pola **Włącz regułę**. Konieczność wyłączenia reguły bez jej usuwania może być w przypadku, gdy chcesz tymczasowo wykluczyć regułę z listy reguł znakowania, a potem będziesz chciał znowu włączyć ją do listy.

Automatyczne znakowanie urządzeń

Możesz tworzyć i modyfikować reguły automatycznego znakowania w oknie właściwości Serwera administracyjnego.

W celu automatycznego znakowania urządzeń:

1. W drzewie konsoli wybierz węzeł z nazwą Serwera administracyjnego, dla którego musisz określić reguły znakowania.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Reguły znakowania**.
4. W sekcji **Reguły znakowania** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Nowa reguła**.

5. W oknie **Nowa reguła** skonfiguruj ogólne właściwości reguły:

   - Określ nazwę reguły.

     Nazwa reguły nie może zawierać więcej niż 255 znaków oraz nie może zawierać żadnych znaków specjalnych (takich jak `"*<>?\:|`).

   - Włącz lub wyłącz regułę, korzystając z pola **Włącz regułę**.

     Domyślnie zaznaczone jest pole **Włącz regułę**.

   - W polu **Znacznik** wprowadź nazwę znacznika.

     Nazwa znacznika nie może zawierać więcej niż 255 znaków oraz nie może zawierać żadnych znaków specjalnych (takich jak `"*<>?\:|`).

6. W sekcji **Warunki** kliknij przycisk **Dodaj**, aby dodać nowy warunek, lub kliknij przycisk **Właściwości**, aby zmodyfikować istniejący warunek.

   Zostanie otwarte okno kreatora nowego warunku reguły automatycznego znakowania.

7. W oknie **Warunek przypisywania znacznika** zaznacz pola obok warunków, które mają mieć wpływ na znakowanie. Możesz określić kilka warunków.

8. W zależności od wybranego warunku przypisywania znaczników, kreator wyświetli okna, w których można skonfigurować odpowiednie warunki. Skonfiguruj wyzwalanie reguły według następujących warunków:

   - **Użycie komputera lub połączenie z określoną siecią**—właściwości sieci urządzenia, takie jak nazwa urządzenia w sieci Windows, a także uwzględnienie urządzenia w domenie lub podsieci IP.

     > Jeśli dla bazy danych używanej z Kaspersky Security Center ustawione jest sortowanie z rozróżnianiem wielkości liter, zachowaj wielkość liter podczas określania nazwy DNS urządzenia. W przeciwnym razie reguła automatycznego tagowania nie będzie działać.

   - **Użycie Active Directory**—obecność urządzenia w jednostce organizacyjnej Active Directory i członkostwo urządzenia w grupie Active Directory.

   - **Określone aplikacje**—obecność Agenta sieciowego na urządzeniu oraz typ, wersja i architektura systemu operacyjnego.

   - **Maszyny wirtualne**—uwzględnienie urządzenia w określonym typie maszyn wirtualnych.

   - **Zainstalowano aplikację z rejestru aplikacji**—obecność aplikacji różnych producentów na urządzeniu.

9. Po skonfigurowaniu warunku, wprowadź jego nazwę, a następnie zamknij okno kreatora.

   Jeśli to konieczne, dla jednej reguły możesz ustawić kilka warunków. W tej sytuacji znacznik zostanie przypisany do urządzenia, jeśli spełnia przynajmniej jeden warunek. Dodane warunki będą wyświetlane w oknie właściwości reguły.

10. Kliknij **OK** w oknie **Nowa reguła**, a następnie kliknij **OK** w oknie właściwości Serwera administracyjnego.

Nowo utworzone reguły są wymuszone na urządzeniach zarządzanych przez wybrany Serwer administracyjny. Jeśli ustawienia urządzenia spełniają warunki reguły, do urządzenia zostanie przydzielony znacznik.

Przeglądanie i konfigurowanie znaczników przydzielonych do urządzenia

Możesz wyświetlić listę wszystkich znaczników, które zostały przypisane do urządzenia, a także przejść do konfiguracji reguł automatycznego znakowania w oknie właściwości urządzenia.

W celu wyświetlenia i skonfigurowania znaczników przypisanych do urządzenia:

1. W drzewie konsoli otwórz folder **Zarządzane urządzenia**.
2. W obszarze roboczym folderu **Zarządzane urządzenia** wybierz urządzenie, dla którego chcesz wyświetlić przypisane znaczniki.
3. Z menu kontekstowego urządzenia mobilnego wybierz **Właściwości**.
4. W oknie właściwości urządzenia wybierz sekcję **Znaczniki**.

   Zostanie wyświetlona lista znaczników przypisanych do wybranego urządzenia, a także sposób, w jaki każdy znacznik został przypisany: ręcznie lub zgodnie z regułą.
5. Jeśli to konieczne, wykonaj następujące czynności:
   - Aby przejść do konfiguracji reguł znakowania, kliknij odnośnik **Ustaw reguły automatycznego znakowania** (tylko dla systemu Windows).
   - Aby zmienić nazwę znacznika, zaznacz go i kliknij przycisk **Zmień nazwę**.
   - Aby usunąć nazwę znacznika, zaznacz go i kliknij przycisk **Usuń**.
   - Aby ręcznie dodać znacznik, wprowadź go w polu znajdującym się w dolnej części sekcji **Znaczniki** i kliknij przycisk **Dodaj**.
6. Jeśli w sekcji **Znaczniki** wprowadziłeś jakiekolwiek zmiany, kliknij przycisk **Zastosuj**, aby te zmiany zostały zastosowane.
7. Kliknij **OK**.

Jeśli we właściwościach urządzenia usunąłeś znacznik lub zmieniłeś jego nazwę, ta zmiana nie będzie wpływać na reguły znakowania, które zostały skonfigurowane we właściwościach Serwera administracyjnego. Zmiana zostanie zastosowana tylko na tym urządzeniu, w którego właściwościach została wprowadzona.

Zdalna diagnostyka urządzeń klienckich. Narzędzie do zdalnej diagnostyki Kaspersky Security Center

Narzędzie do zdalnej diagnostyki programu Kaspersky Security Center (zwane dalej narzędziem do zdalnej diagnostyki) zostało zaprojektowane do zdalnego wykonywania na urządzeniach klienckich następujących działań:

- Włączania i wyłączania śledzenia, zmieniania poziomu śledzenia, pobierania pliku śledzenia.
- Pobierania informacji o systemie i ustawień aplikacji.
- Pobierania dzienników zdarzeń.
- Generowania pliku zrzutu dla aplikacji.
- Uruchamiania diagnostyki i pobierania jej raportów.
- Uruchamiania i zatrzymywania działania aplikacji.

Możesz użyć dzienników zdarzeń i raportów diagnostycznych pobranych z urządzenia klienckiego do samodzielnego rozwiązania problemów. Dodatkowo, specjalista z działu pomocy technicznej Kaspersky może poprosić o pobranie plików śledzenia, plików zrzutu pamięci, dzienników zdarzeń, a także raportów diagnostycznych z urządzenia klienckiego w celu przeprowadzenia dalszej analizy w Kaspersky.

Narzędzie do zdalnej diagnostyki jest automatycznie instalowane na urządzeniu wraz z Konsolą administracyjną.

Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim

W celu połączenia narzędzia do zdalnej diagnostyki z urządzeniem klienckim:

1. Z drzewa konsoli wybierz dowolną grupę administracyjną.
2. W obszarze roboczym, na zakładce **Urządzenia**, z menu kontekstowego dowolnego urządzenia wybierz **Narzędzia użytkownika → Zdalna diagnostyka**.

   Zostanie otwarte okno główne narzędzia do zdalnej diagnostyki.
3. W pierwszym polu okna głównego narzędzia do zdalnej diagnostyki określ narzędzia, których chcesz użyć do nawiązania połączenia z urządzeniem:

   - **Dostęp przy użyciu sieci Microsoft Windows**.
   - **Dostęp przy użyciu Serwera administracyjnego**.
4. Jeżeli w pierwszym polu okna głównego narzędzia zaznaczyłeś opcję **Dostęp przy użyciu sieci Microsoft Windows**, wykonaj następujące czynności:

   - W polu **Urządzenie** określ adres urządzenia, z którym chcesz się połączyć

     Jako adresu urządzenia użyj adresu IP, nazwy NetBIOS lub nazwy DNS.

     Domyślną wartością jest adres urządzenia, z którego menu kontekstowego uruchomiono narzędzie.
   - Określ konto, z którego nawiązywane jest połączenie z urządzeniem:

     - **Połącz jako bieżący użytkownik** (wybrane domyślnie). Nawiąż połączenie, korzystając z konta bieżącego użytkownika.
     - **Do połączenia użyj nazwy użytkownika i hasła**. Nawiąż połączenie, korzystając z określonego konta użytkownika. Określ **Nazwę użytkownika** i **Hasło** żądanego konta.

     Połączenie z urządzeniem jest możliwe tylko z poziomu konta lokalnego administratora urządzenia.
5. Jeżeli w pierwszym polu okna głównego narzędzia zaznaczyłeś opcję **Dostęp przy użyciu Serwera administracyjnego**, wykonaj następujące czynności:

   - W polu **Serwer administracyjny** określ adres Serwera administracyjnego, z którego zamierzasz połączyć się z urządzeniem.

     Jako adresu serwera użyj adresu IP, nazwy NetBIOS lub nazwy DNS.

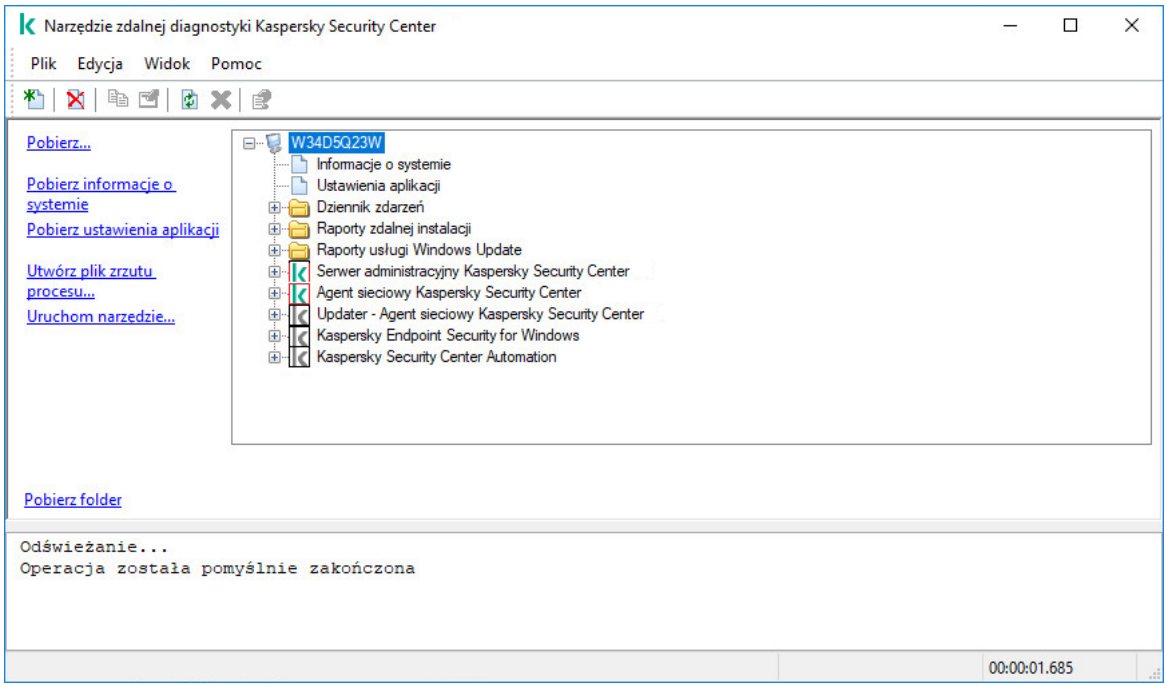
     Domyślną wartością jest adres Serwera administracyjnego, z którego uruchomiono narzędzie.
   - Jeśli jest to wymagane, zaznacz pola **Użyj SSL**, **Kompresuj ruch** oraz **Urządzenie należy do podrzędnego Serwera administracyjnego**.

Jeżeli zaznaczone jest pole **Urządzenie należy do podrzędnego Serwera administracyjnego**, w polu **Urządzenie należy do podrzędnego Serwera administracyjnego** możesz podać nazwę podrzędnego Serwera administracyjnego, który zarządza urządzeniem, klikając przycisk **Przeglądaj**.

6. Aby połączyć się z urządzeniem, kliknij przycisk **Zaloguj się**.

Możesz przeprowadzić autoryzację z użyciem weryfikacji dwuetapowej, jeśli jest ona włączona dla Twojego konta.

Zostanie otwarte okno przeznaczone do zdalnej diagnostyki urządzenia (patrz rysunek poniżej). Lewa część okna zawiera odnośniki do działań diagnostyki urządzenia. W prawej części okna znajduje się drzewo obiektów urządzenia, którymi może zarządzać narzędzie. Dolna część okna wyświetla postęp wykonywania działań narzędzia.



Narzędzie do zdalnej diagnostyki. Okno Zdalna diagnostyka urządzeń

Narzędzie do zdalnej diagnostyki zapisuje pliki pobrane z urządzeń na pulpicie urządzenia, z którego zostało uruchomione.

Włączanie i wyłączanie śledzenia, pobieranie pliku śledzenia

W celu włączenia śledzenia na zdalnym urządzeniu:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem.

2. Z drzewa obiektów urządzenia wybierz aplikację, dla której chcesz włączyć śledzenie.

Śledzenie może być włączane i wyłączane dla aplikacji posiadających funkcję autoochrony tylko wtedy, gdy urządzenie jest połączone przy użyciu narzędzi Serwera administracyjnego.

Jeśli chcesz włączyć śledzenie dla Agenta sieciowego, możesz to zrobić podczas tworzenia zadania Zainstaluj wymagane aktualizacje i napraw luki. W tym przypadku Agent sieciowy zapisze informacje o śledzeniu nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w narzędziu do zdalnej diagnostyki.

3. W celu włączenia śledzenia:

   a. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Włącz śledzenie**.

   b. W otwartym oknie **Wybierz poziom śledzenia** zalecane jest zachowanie domyślnych wartości ustawień. Jeśli jest to wymagane, specjalista z pomocy technicznej przeprowadzi Cię przez proces konfiguracji. Dostępne są następujące ustawienia:

   - Poziom śledzenia

     Poziom śledzenia definiuje ilość szczegółów, jaką plik śledzenia zawiera.

   - Śledzenie na podstawie rotacji (dostępne tylko dla Kaspersky Endpoint Security)

     Aplikacja nadpisuje informacje o śledzeniu, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Określ maksymalną liczbę plików, jaka będzie używana do przechowywania informacji o śledzeniu, a także maksymalny rozmiar każdego pliku. Jeśli zostanie zapisana maksymalna liczba plików śledzenia o maksymalnym rozmiarze, najstarszy plik śledzenia zostanie usunięty, aby mógł zostać zapisany nowy plik śledzenia.

   c. Kliknij **OK**.

4. W przypadku Kaspersky Endpoint Security specjalista z pomocy technicznej może poprosić o włączenie śledzenia Xperf dla informacji o działaniu systemu.

   W celu włączenia śledzenia Xperf:

   a. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Włącz śledzenie Xperf**.

   b. W otwartym oknie **Wybierz poziom śledzenia**, w zależności od odpowiedzi od specjalisty z pomocy technicznej, wybierz jeden z następujących poziomów śledzenia:

   - Niski

     Plik śledzenia tego typu zawiera minimalną ilość informacji o systemie.

     Domyślnie opcja ta jest zaznaczona.

   - Głęboki

     Plik śledzenia tego typu zawiera bardziej szczegółowe informacje niż pliki śledzenia typu *Niski* i specjaliści z pomocy technicznej mogą poprosić o nie, gdy plik śledzenia typu *Niski* nie jest wystarczający do oceny działania. *Głęboki* plik śledzenia zawiera informacje techniczne o systemie, w tym informacje o sprzęcie, systemie operacyjnym, listę uruchomionych i zakończonych procesów i aplikacji, zdarzeń użytych do oceny działania, a także zdarzeń z Narzędzia do oceny wydajności systemu Windows.

   c. Wybierz jeden z następujących typów śledzenia:

   - Podstawowy

Informacje o śledzeniu są otrzymywane podczas działania aplikacji Kaspersky Endpoint Security.

Domyślnie opcja ta jest zaznaczona.

- Po ponownym uruchomieniu

  Informacje o śledzeniu są otrzymywane, gdy system operacyjny jest uruchamiany na zarządzanym urządzeniu. Ten typ śledzenia jest efektywny, gdy problem, który wpływa na działanie systemu, pojawi się po włączeniu urządzenia, a przed uruchomieniem Kaspersky Endpoint Security.

d. Możesz także zostać poproszony o włączenie opcji **Śledzenie na podstawie rotacji**, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Następnie określ maksymalny rozmiar pliku śledzenia. Jeśli plik osiągnie maksymalny rozmiar, najstarsze informacje śledzenia zostaną nadpisane nowymi informacjami.

e. Kliknij **OK**.

W niektórych przypadkach, aby włączyć śledzenie, konieczne jest ponowne uruchomienie aplikacji zabezpieczającej i jej zadania.

Narzędzie do zdalnej diagnostyki włączy śledzenie wybranej aplikacji.

W celu pobrania pliku śledzenia aplikacji:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".
2. W węźle aplikacji, w folderze **Pliki śledzenia** wybierz żądany plik.
3. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Pobierz cały plik**.

   W przypadku plików o dużym rozmiarze można pobrać ich ostatnio utworzone części.

   Podświetlony plik śledzenia może zostać usunięty. Plik może zostać usunięty po wyłączeniu śledzenia.

Wybrany plik jest pobierany do lokalizacji określonej w dolnej części okna.

W celu wyłączenia śledzenia na zdalnym urządzeniu:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".
2. W drzewie obiektów urządzenia wybierz aplikację, dla której chcesz wyłączyć śledzenie.

   Śledzenie może być włączane i wyłączane dla aplikacji posiadających funkcję autoochrony tylko wtedy, gdy urządzenie jest połączone przy użyciu narzędzi Serwera administracyjnego.

3. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Wyłącz śledzenie**.

Narzędzie do zdalnej diagnostyki wyłączy śledzenie wybranej aplikacji.

Pobierania ustawień aplikacji

W celu pobrania ustawień aplikacji ze zdalnego urządzenia:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. W drzewie obiektów okna narzędzia do zdalnej diagnostyki wybierz węzeł z nazwą urządzenia, znajdujący się na najwyższej pozycji.

3. W lewej części okna narzędzia do zdalnej diagnostyki wybierz żądane działanie z następujących opcji:

   - **Pobierz informacje o systemie**
   - **Pobierz ustawienia aplikacji**
   - **Utwórz plik zrzutu procesu**

     W oknie, które zostanie otwarte po kliknięciu tego odnośnika, określ plik wykonywalny aplikacji, dla której chcesz wygenerować plik zrzutu pamięci.

   - **Uruchom narzędzie**

     W oknie, które zostanie otwarte po kliknięciu tego odnośnika, określ plik wykonywalny narzędzia, które chcesz uruchomić, oraz ustawienia jego uruchamiania.

Narzędzie zostanie pobrane i uruchomione na urządzeniu.

Pobierania dzienników zdarzeń

W celu pobrania dziennika zdarzeń ze zdalnego urządzenia:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. W folderze **Dzienniki zdarzeń systemowych** drzewa obiektów urządzenia wybierz odpowiedni raport.

3. Pobierz wybrany dziennik, klikając odnośnik **Pobierz dziennik zdarzeń <nazwa dziennika zdarzeń>** w lewej części okna narzędzia do zdalnej diagnostyki.

Wybrany dziennik zdarzeń jest pobierany do lokalizacji określonej w dolnym panelu.

Pobieranie kilku elementów informacji diagnostycznych

Narzędzie do zdalnej diagnostyki Kaspersky Security Center umożliwia pobranie kilku elementów informacji diagnostycznych, w tym dzienników zdarzeń, informacji o systemie, plików śledzenia i plików zrzutów.

W celu pobrania informacji diagnostycznych ze zdalnego urządzenia:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".

2. W lewej części okna narzędzia do zdalnej diagnostyki kliknij **Pobierz**.

3. Zaznacz pola obok elementów, które chcesz pobrać.

4. Kliknij **Uruchom**.

Każdy wybrany element zostanie pobrany do lokalizacji określonej w dolnym panelu.

Uruchamianie diagnostyki i pobieranie wyników

W celu uruchomienia diagnostyki aplikacji na zdalnym urządzeniu i pobrania wyników:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".
2. Z drzewa obiektów urządzenia wybierz żądaną aplikację.
3. Uruchom diagnostykę, klikając odnośnik **Uruchom diagnostykę**, dostępny w lewej części okna narzędzia do zdalnej diagnostyki.

   W drzewie obiektów, w węźle wybranej aplikacji pojawi się raport z diagnostyki.
4. W drzewie obiektów wybierz nowo utworzony raport z diagnostyki i pobierz go, klikając odnośnik **Pobierz folder**.

Wybrany raport jest pobierany do lokalizacji określonej w dolnym panelu.

Uruchamianie, zatrzymywanie i ponowne uruchamianie aplikacji

Aplikacje mogą być uruchamiane, zatrzymywane i ponownie uruchamiane tylko wtedy, gdy połączyłeś urządzenie przy użyciu narzędzi Serwera administracyjnego.

W celu uruchomienia, zatrzymania lub ponownego uruchomienia aplikacji:

1. Uruchom narzędzie do zdalnej diagnostyki i połącz je z żądanym urządzeniem tak, jak opisano to w sekcji „Łączenie narzędzia do zdalnej diagnostyki z urządzeniem klienckim".
2. Z drzewa obiektów urządzenia wybierz żądaną aplikację.
3. W lewej części okna narzędzia do zdalnej diagnostyki wybierz działanie:
   - **Zatrzymaj aplikację**
   - **Uruchom aplikację ponownie**
   - **Uruchom aplikację**

W zależności od wybranej akcji, aplikacja zostanie uruchomiona, zatrzymana lub uruchomiona ponownie.

Urządzenia chronione UEFI

Urządzenie chronione UEFI z programem Kaspersky Anti-Virus dla UEFI zintegrowanym na poziomie BIOS-u. Zintegrowana ochrona zapewnia bezpieczeństwo urządzenia od momentu uruchomienia systemu, natomiast ochrona na urządzeniach bez zintegrowanego oprogramowania zaczyna działać dopiero po uruchomieniu aplikacji zabezpieczającej. Kaspersky Security Center obsługuje zarządzanie tymi urządzeniami.

W celu zmodyfikowania ustawień połączenia urządzeń chronionych UEFI:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego wybierz **Ustawienia połączenia z serwerem** → **Porty dodatkowe**.
4. W sekcji **Porty dodatkowe** zmodyfikuj odpowiednie ustawienia:
   - Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS

     Urządzenia chronione UEFI mogą nawiązywać połączenie z Serwerem administracyjnym.

   - Port dla urządzeń chronionych UEFI i urządzeń KasperskyOS

     Możesz zmienić numer portu, jeśli opcja **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS** jest włączona. Domyślny numer portu to 13294.
5. Kliknij **OK**.

Ustawienia zarządzanego urządzenia

W celu sprawdzenia ustawień zarządzanego urządzenia:

1. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
2. W obszarze roboczym folderu wybierz urządzenie.
3. Z otwartego menu kontekstowego urządzenia wybierz **Właściwości**.

Zostanie otwarte okno właściwości wybranego urządzenia z wybraną sekcją **Ogólny**.

Ogólne

Sekcja **Ogólny** wyświetla ogólne informacje o urządzeniu klienckim. Informacje są dostarczane w oparciu o dane otrzymane podczas ostatniej synchronizacji urządzenia klienckiego z Serwerem administracyjnym:

- Nazwa

  W tym polu możesz wyświetlić i zmodyfikować nazwę urządzenia klienckiego w grupie administracyjnej.

- Opis

  W tym polu możesz wprowadzić dodatkowy opis urządzenia klienckiego.

- Domena Windows

Domena lub grupa robocza Windows, która zawiera urządzenie.

- **Nazwa NetBIOS**

  Nazwa urządzenia klienckiego w sieci Windows.

- **Nazwa DNS**

  Nazwa domeny DNS urządzenia klienckiego.

- **Adres IP**

  Adres IP urządzenia.

- **Grupa**

  Grupa administracyjna zawierająca urządzenie klienckie.

- **Ostatnia aktualizacja**

  Data ostatniej aktualizacji antywirusowych baz danych lub aplikacji na urządzeniu.

- **Ostatnio dostępny**

  Data i godzina, gdy urządzenie było ostatnio widoczne w sieci.

- **Połączono z Serwerem administracyjnym**

  Data i godzina ostatniego połączenia Agenta sieciowego, zainstalowanego na urządzeniu klienckim, z Serwerem administracyjnym.

- **Nie odłączaj od Serwera administracyjnego**

  Jeśli ta opcja jest włączona, utrzymywana jest ciągła łączność pomiędzy zarządzanym urządzeniem a Serwerem administracyjnym. Możesz użyć tej opcji, jeśli nie używasz serwerów push, które zapewniają taką łączność.

  Jeśli ta opcja jest wyłączona, a serwery push nie są używane, zarządzane urządzenie będzie nawiązywało połączenie z Serwerem administracyjnym jedynie w celu synchronizacji danych lub przesłania informacji.

  Maksymalna całkowita liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego** to 300.

  Ta opcja jest wyłączona domyślnie na zarządzanych urządzeniach. Ta opcja jest włączona domyślnie na urządzeniu, na którym jest zainstalowany Serwer administracyjny i pozostaje włączona nawet w przypadku próby jej wyłączenia.

Ochrona

Sekcja **Ochrona** zawiera informacje o bieżącym stanie ochrony antywirusowej na urządzeniu klienckim:

- **Stan urządzenia**

  Stan urządzenia klienckiego przypisany w oparciu o kryteria zdefiniowane przez administratora dla stanu ochrony antywirusowej na urządzeniu i aktywności urządzenia w sieci.

- **Wszystkie problemy**

  Ta tabela zawiera pełną listę problemów wykrytych przez zarządzane aplikacje zainstalowane na urządzeniu klienckim. Każdemu problemowi towarzyszy stan, który aplikacja sugeruje przypisać do urządzenia dla tego problemu.

- **Ochrona w czasie rzeczywistym**

  To pole wyświetla bieżący stan ochrony urządzenia klienckiego w czasie rzeczywistym.

  Jeśli stan zmieni się na urządzeniu, nowy stan zostanie wyświetlony w oknie właściwości urządzenia dopiero po zsynchronizowaniu urządzenia klienckiego z Serwerem administracyjnym.

- **Ostatnie skanowanie na żądanie**

  Data i godzina ostatniego skanowania w poszukiwaniu złośliwego oprogramowania przeprowadzonego na urządzeniu klienckim.

- **Łączna liczba wykrytych zagrożeń**

  Całkowita liczba zagrożeń wykrytych na urządzeniu klienckim od momentu zainstalowania aplikacji antywirusowej (pierwsze skanowanie) lub od momentu ostatniego zresetowania licznika zagrożeń.

- **Aktywne zagrożenia**

  Liczba nieprzetworzonych plików na urządzeniu klienckim.

  To pole ignoruje liczbę nieprzetworzonych plików na urządzeniach mobilnych.

- **Stan szyfrowania dysku**

  Bieżący stan szyfrowania plików na lokalnych dyskach urządzenia. Opis statusów znajduje się w pomocy Kaspersky Endpoint Security for Windows.

Aplikacje

Sekcja **Aplikacje** wyświetla wszystkie aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim:

- **Zdarzenia**

  Kliknięcie tego przycisku wyświetla listę zdarzeń, które wystąpiły na urządzeniu klienckim podczas działania aplikacji, oraz wyświetla wyniki zadania dla tej aplikacji.

- Statystyki

  Kliknięcie tego przycisku wyświetla bieżące informacje statystyczne dotyczące aplikacji.

- Właściwości

  Po kliknięciu tego przycisku można zobaczyć informacje o aplikacji oraz skonfigurować aplikację.

Zadania

W zakładce **Zadania** możesz zarządzać zadaniami urządzenia klienckiego: przeglądać listę istniejących zadań, tworzyć nowe zadania, usuwać, uruchamiać i zatrzymywać zadania, a także modyfikować ustawienia zadań i przeglądać wyniki ich wykonania. Lista zadań jest tworzona w oparciu o dane otrzymane w czasie ostatniej synchronizacji komputera klienckiego z Serwerem administracyjnym. Serwer administracyjny żąda od urządzenia klienckiego szczegółów dotyczących stanu zadania. Jeśli połączenie nie jest nawiązane, stan nie jest wyświetlany.

Zdarzenia

Zakładka **Zdarzenia** wyświetla zdarzenia zarejestrowane na Serwerze administracyjnym dla wybranego urządzenia klienckiego.

Znaczniki

W zakładce **Znaczniki** możesz zarządzać listą słów kluczowych, które są używane podczas wyszukiwania urządzeń klienckich: przejrzeć listę istniejących znaczników, przypisać znaczniki z listy, skonfigurować reguły automatycznego oznaczania oraz dodać nowe znaczniki i zmienić nazwy starszych znaczników, a także usunąć znaczniki.

Informacje o systemie

Sekcja **Ogólne informacje o systemie** zawiera informacje o aplikacji zainstalowanej na urządzeniu klienckim.

Rejestr aplikacji

W sekcji **Rejestr aplikacji** możesz przejrzeć rejestr aplikacji zainstalowanych na urządzeniu klienckim i ich uaktualnień, a także możesz skonfigurować wyświetlanie rejestru aplikacji.

Informacje o zainstalowanych aplikacjach są dostępne, jeśli Agent sieciowy zainstalowany na urządzeniu klienckim prześle żądane informacje do Serwera administracyjnego. Możesz skonfigurować przesyłanie informacji do Serwera administracyjnego w oknie właściwości Agenta sieciowego lub jego zasady, w sekcji **Repozytoria**. Informacje o zainstalowanych aplikacjach są dostarczane tylko dla urządzeń działających pod kontrolą systemu Windows.

Agent sieciowy dostarcza informacje o aplikacjach w oparciu o dane pobrane z rejestru systemu.

- Wyświetl tylko niekompatybilne aplikacje zabezpieczające

Jeśli ta opcja jest włączona, lista aplikacji zawiera tylko te aplikacje zabezpieczające, które są niekompatybilne z aplikacjami firmy Kaspersky.

Domyślnie opcja ta jest wyłączona.

- **Pokaż uaktualnienia**

  Jeśli ta opcja jest włączona, lista aplikacji zawiera nie tylko aplikacje, ale także zainstalowane dla nich pakiety aktualizacyjne.

  Aby wyświetlić listę aktualizacji, potrzebne jest 100 KB ruchu. Jeśli zamkniesz listę i otworzysz ją ponownie, będziesz musiał ponownie poświęcić 100 KB ruchu internetowego.

  Domyślnie opcja ta jest wyłączona.

- **Eksportuj do pliku**

  Kliknij ten przycisk, aby wyeksportować listę aplikacji zainstalowanych na urządzeniu do pliku CSV lub TXT.

- **Historia**

  Kliknij ten przycisk, aby przejrzeć zdarzenia dotyczące instalacji aplikacji na urządzeniu. Wyświetlane są następujące informacje:

  - Data i godzina zainstalowania aplikacji na urządzeniu
  - Nazwa aplikacji
  - Wersja aplikacji

- **Właściwości**

  Kliknij ten przycisk, aby przejrzeć właściwości aplikacji wybranej na liście aplikacji zainstalowanych na urządzeniu. Wyświetlane są następujące informacje:

  - Nazwa aplikacji
  - Wersja aplikacji
  - Producent aplikacji

Pliki wykonywalne

Sekcja **Pliki wykonywalne** wyświetla pliki wykonywalne wykryte na urządzeniu klienckim.

Rejestrze sprzętu

W sekcji **Rejestr sprzętu** możesz wyświetlić informacje o sprzęcie zainstalowanym na urządzeniu klienckim. Możesz przejrzeć informacje dla urządzeń z systemem Windows oraz urządzeń z systemem Linux.

Sesje

Sekcja **Sesje** wyświetla informacje o właścicielu urządzenia klienckiego, a także o kontach użytkowników, którzy pracowali na wybranym urządzeniu klienckim.

Informacje o użytkownikach domeny są generowane w oparciu o dane Active Directory. Szczegóły dotyczące użytkowników lokalnych są dostępne w Menedżerze konta zabezpieczeń Windows, zainstalowanym na urządzeniu klienckim.

- **Właściciel urządzenia**

  Pole **Właściciel urządzenia** wyświetla nazwę użytkownika, z którym administrator może się skontaktować, gdy zajdzie potrzeba wykonania określonych działań na urządzeniu klienckim.

  Użyj przycisków **Przypisz** i **Właściwości**, aby wybrać właściciela urządzenia oraz wyświetlić informacje o użytkowniku, który został wskazany jako właściciel urządzenia.

  Użyj przycisku z czerwonym krzyżykiem, aby usunąć aktualnego właściciela urządzenia.

Lista wyświetla konta użytkowników, którzy korzystają z urządzenia klienckiego.

- **Nazwa**

  Nazwa urządzenia w sieci Windows.

- **Nazwa uczestnika**

  Nazwa (domena lub nazwa lokalna) użytkownika, który logował się do systemu tego urządzenia.

- **Konto**

  Konto użytkownika, który logował się na tym urządzeniu.

- **E-mail**

  Adres e-mail użytkownika.

- **Telefon**

  Numer telefonu użytkownika.

Zdarzenia

W zakładce **Incydenty** możesz przejrzeć, zmodyfikować i utworzyć zdarzenia dla urządzenia klienckiego. Zdarzenia mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora. Na przykład, jeśli niektórzy użytkownicy regularnie przenoszą szkodliwe programy ze swoich nośników wymiennych na urządzenia, administrator może utworzyć zdarzenie. W treści zdarzenia administrator może dostarczyć krótki opis zdarzenia oraz zalecane działania (na przykład działania dyscyplinarne wobec użytkownika), a także dodać odsyłacz.

Zdarzenie, dla którego zostały wykonane wszystkie zalecane działania, nazywane jest *przetworzonym*. Obecność nieprzetworzonych zdarzeń może zostać wybrana jako warunek zmiany stanu urządzenia na *Krytyczny* lub *Ostrzeżenie*.

Ta sekcja zawiera listę zdarzeń, które zostały utworzone dla urządzenia. Zdarzenia są klasyfikowane według priorytetu i typu. Typ zdarzenia jest definiowany przez aplikację Kaspersky, która utworzyła zdarzenie. Możesz podświetlić przetworzone zdarzenia na liście, zaznaczając pole w kolumnie **Przetworzone**.

Luki w oprogramowaniu

Sekcja **Luki w oprogramowaniu** zawiera informacje o lukach w aplikacjach firm trzecich zainstalowanych na urządzeniach klienckich. Do wyszukiwania luk po nazwie możesz użyć pola wyszukiwania znajdującego się nad listą.

- **Eksportuj do pliku**

  Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę luk do pliku. Domyślnie aplikacja eksportuje listę luk do pliku CSV.

- **Pokaż tylko luki, które można naprawić**

  Jeśli ta opcja jest włączona, sekcja wyświetla luki, które można naprawić przy użyciu poprawki.

  Jeśli ta opcja jest wyłączona, sekcja wyświetla luki, które można wyeliminować przy użyciu poprawki, oraz luki, dla których nie opublikowano poprawki.

  Domyślnie opcja ta jest włączona.

- **Właściwości**

  Na liście wybierz lukę w oprogramowaniu i kliknij przycisk **Właściwości**, aby przejrzeć właściwości wybranej luki w oprogramowaniu w oddzielnym oknie. W oknie możesz wykonać następujące czynności:

  - Zignoruj lukę w oprogramowaniu na tym zarządzanym urządzeniu (w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console).
  - Przejrzyj listę zalecanych poprawek dla luki.
  - Ręcznie określ aktualizacje oprogramowania, aby naprawić lukę (w Konsoli administracyjnej lub w Kaspersky Security Center Web Console).
  - Przejrzyj instancje luki.
  - Przejrzyj listę istniejących zadań, aby naprawić lukę i utworzyć nowe zadania w celu wyeliminowania luki.

Dostępne aktualizacje

Sekcja ta wyświetla listę aktualizacji oprogramowania znajdujących się na tym urządzeniu, ale jeszcze nie zainstalowanych.

- **Pokaż zainstalowane aktualizacje**

Jeśli ta opcja jest włączona, lista wyświetla uaktualnienia, które nie zostały zainstalowane oraz te, które zostały już zainstalowane na urządzeniu klienckim.

Domyślnie opcja ta jest wyłączona.

Zasady aktywne

Ta sekcja wyświetla listę zasad aplikacji firmy Kaspersky aktualnie aktywnych na tym urządzeniu.

- **Eksportuj do pliku**

  Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę aktywnych zasad do pliku. Domyślnie aplikacja eksportuje listę zasad do pliku CSV.

Aktywne profile zasad

- **Aktywne profile zasad**

  Lista umożliwia przejrzenie informacji o istniejących profilach zasad, które są aktywne na urządzeniach klienckich. Aby odszukać aktywne profile zasad na liście, można użyć paska wyszukiwania znajdującego się nad listą, w którym należy wprowadzić nazwę zasady lub nazwę profilu zasad.

- **Eksportuj do pliku**

  Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę aktywnych profili zasad do pliku. Domyślnie aplikacja eksportuje listę profili zasad do pliku CSV.

Punkty dystrybucji

Ta sekcja zawiera listę punktów dystrybucji, z którymi urządzenie komunikuje się.

- **Eksportuj do pliku**

  Kliknij przycisk **Eksportuj do pliku**, aby zapisać do pliku listę punktów dystrybucji, z którymi urządzenie komunikuje się. Domyślnie aplikacja eksportuje listę urządzeń do pliku CSV.

- **Właściwości**

  Kliknij przycisk **Właściwości**, aby przejrzeć i skonfigurować punkt dystrybucji, z którym urządzenie komunikuje się.

Ogólne ustawienia zasady

Ogólny

W sekcji **Ogólny** możesz zmodyfikować stan zasady oraz określić dziedziczenie ustawień zasady:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:
  - Zasada aktywna

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.

  - Zasada użytkownika mobilnego

    Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.

  - Zasada nieaktywna

    Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.

- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:
  - Dziedzicz ustawienia z zasady nadrzędnej

    Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

    Domyślnie opcja ta jest włączona.

  - Wymuś dziedziczenie ustawień w zasadach podrzędnych

    Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:

    - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.
    - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

    Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

    Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Sekcja **Konfiguracja zdarzenia** umożliwia skonfigurowanie zapisywania zdarzeń oraz powiadamiania o zdarzeniach. Zdarzenia są grupowane według istotności na następujących zakładkach:

- **Krytyczny**

  Zakładka **Krytyczny** nie jest wyświetlana we właściwościach zasady Agenta sieciowego.

- **Błąd funkcjonalny**

- **Ostrzeżenie**
- **Informacja**

Na każdej zakładce, lista wyświetla typy zdarzeń oraz domyślny okres przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Kliknięcie przycisku **Właściwości** umożliwia określenie ustawień zapisywania zdarzeń oraz powiadomień o zdarzeniach wybranych z listy. Domyślnie, podstawowe ustawienia powiadamiania, określone dla całego Serwera administracyjnego, są używane dla wszystkich typów zdarzeń. Jednakże możesz zmienić określone ustawienia dla żądanych typów zdarzeń.

Na przykład, na zakładce **Ostrzeżenie** możesz skonfigurować typ zdarzenia **Wystąpił incydent**. Takie zdarzenia mogą mieć miejsce, na przykład, gdy wolne miejsce na dysku punktu dystrybucji jest mniejsze niż 2 GB (co najmniej 4 GB są wymagane do zdalnego instalowania aplikacji i pobierania aktualizacji). Aby skonfigurować zdarzenie **Wystąpił incydent**, wybierz je i kliknij przycisk **Właściwości**. Następnie możesz określić, gdzie mają być przechowywane zdarzenia i jak o nich powiadamiać.

Jeśli Agent sieciowy wykrył incydent, możesz nim zarządzać za pomocą ustawień zarządzanego urządzenia.

Aby wybrać kilka typów zdarzeń, użyj klawisza **Shift** lub **Ctrl**; aby wybrać wszystkie typy, użyj przycisku **Wybierz wszystkie**.

Ustawienia zasady Agenta sieciowego

W celu skonfigurowania zasady Agenta sieciowego:

1. Z drzewa konsoli wybierz folder **Zasady**.
2. W obszarze roboczym folderu wybierz zasadę Agenta sieciowego.
3. Z otwartego menu kontekstowego zasady wybierz **Właściwości**.

Zostanie otwarte okno właściwości zasady Agenta sieciowego.

Ogólny

W sekcji **Ogólny** możesz zmodyfikować stan zasady oraz określić dziedziczenie ustawień zasady:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:
  - **Zasada aktywna**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.

  - **Zasada użytkownika mobilnego**

    Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.

  - **Zasada nieaktywna**

Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.

- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:
  - Dziedzicz ustawienia z zasady nadrzędnej

    Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

    Domyślnie opcja ta jest włączona.

  - Wymuś dziedziczenie ustawień w zasadach podrzędnych

    Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:
    - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.
    - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

    Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

    Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Sekcja **Konfiguracja zdarzenia** umożliwia skonfigurowanie zapisywania zdarzeń oraz powiadamiania o zdarzeniach. Zdarzenia są grupowane według istotności na następujących zakładkach:

- **Krytyczny**

  Zakładka **Krytyczny** nie jest wyświetlana we właściwościach zasady Agenta sieciowego.

- **Błąd funkcjonalny**
- **Ostrzeżenie**
- **Informacja**

Na każdej zakładce, lista wyświetla typy zdarzeń oraz domyślny okres przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Kliknięcie przycisku **Właściwości** umożliwia określenie ustawień zapisywania zdarzeń oraz powiadomień o zdarzeniach wybranych z listy. Domyślnie, podstawowe ustawienia powiadamiania, określone dla całego Serwera administracyjnego, są używane dla wszystkich typów zdarzeń. Jednakże możesz zmienić określone ustawienia dla żądanych typów zdarzeń.

Na przykład, na zakładce **Ostrzeżenie** możesz skonfigurować typ zdarzenia **Wystąpił incydent**. Takie zdarzenia mogą mieć miejsce, na przykład, gdy wolne miejsce na dysku punktu dystrybucji jest mniejsze niż 2 GB (co najmniej 4 GB są wymagane do zdalnego instalowania aplikacji i pobierania aktualizacji). Aby skonfigurować zdarzenie **Wystąpił incydent**, wybierz je i kliknij przycisk **Właściwości**. Następnie możesz określić, gdzie mają być przechowywane zdarzenia i jak o nich powiadamiać.

Jeśli Agent sieciowy wykrył incydent, możesz nim zarządzać za pomocą ustawień zarządzanego urządzenia.

Aby wybrać kilka typów zdarzeń, użyj klawisza **Shift** lub **Ctrl**; aby wybrać wszystkie typy, użyj przycisku **Wybierz wszystkie**.

Ustawienia

W sekcji **Ustawienia** możesz skonfigurować zasadę Agenta sieciowego:

- **Rozsyłaj pliki tylko poprzez punkty dystrybucji**

  Jeśli ta opcja jest włączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia tylko z punktów dystrybucji.

  Jeśli ta opcja jest wyłączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia z punktów dystrybucji lub z Serwera administracyjnego.

  Należy pamiętać, że aplikacje zabezpieczające na zarządzanych urządzeniach pobierają uaktualnienia ze źródła ustawionego w zadaniu aktualizacji dla każdej aplikacji zabezpieczającej. Jeśli włączysz opcję **Rozsyłaj pliki tylko poprzez punkty dystrybucji**, upewnij się, że Kaspersky Security Center jest ustawiony jako źródło uaktualnień w zadaniach aktualizacji.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar kolejki zdarzeń, w MB**

  W tym polu możesz określić maksymalny rozmiar przestrzeni dyskowej zajmowanej przez kolejkę zdarzenia.

  Domyślna wartość to 2 megabajty (MB).

- **Aplikacja może pobierać rozszerzone dane zasad na urządzenie**

  Agent sieciowy zainstalowany na zarządzanym urządzeniu przesyła informacje o zastosowanej zasadzie aplikacji zabezpieczającej (na przykład, Kaspersky Endpoint Security for Windows). Przesłane informacje możesz przejrzeć w interfejsie aplikacji zabezpieczającej.

  Agent sieciowy przesyła następujące informacje:

  - Czas dostarczenia zasady na zarządzane urządzenie
  - Nazwę aktywnej zasady lub zasady użytkownika mobilnego w momencie dostarczenia zasady na zarządzane urządzenie
  - Nazwę i pełną ścieżkę do grupy administracyjnej, która zawierała zarządzane urządzenie w momencie dostarczenia zasady na zarządzane urządzenie
  - Lista aktywnych profili zasad

    Możesz użyć informacji, aby zapewnić, że poprawna zasada zostanie zastosowana do urządzenia oraz aby rozwiązać problemy. Domyślnie opcja ta jest wyłączona.

- **Chroń usługę Agenta sieciowego przed nieuprawnionym usuwaniem, zatrzymywaniem i zmianami ustawień**

Po zainstalowaniu Agenta sieciowego na zarządzanym urządzeniu, komponent nie może zostać usunięty ani ponownie skonfigurowany bez żądanych uprawnień. Usługa Agenta sieciowego nie może zostać zatrzymana.

Domyślnie opcja ta jest wyłączona.

- Użyj hasła dezinstalacyjnego

  Jeśli ta opcja jest włączona, klikając przycisk **Modyfikuj**, można określić hasło do zdalnej dezinstalacji Agenta sieciowego.

  Domyślnie opcja ta jest wyłączona.

Repozytoria

W sekcji **Repozytoria** możesz wybrać typy obiektów, których szczegóły zostaną wysłane z Agenta sieciowego na Serwer administracyjny. Jeśli modyfikacja niektórych ustawień w tej sekcji jest zablokowana przez zasadę Agenta sieciowego, nie można ich modyfikować. Ustawienia w sekcji **Repozytoria** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows:

- Szczegóły aktualizacji Windows Update

  Jeśli ta opcja jest włączona, informacje o aktualizacjach Microsoft Windows Update, które powinny zostać zainstalowane na urządzeniach klienckich, są przesyłane do Serwera administracyjnego.

  Czasami, nawet wtedy, gdy opcja jest wyłączona, aktualizacje są wyświetlanie we właściwościach urządzenia w sekcji **Dostępne aktualizacje**. To może mieć miejsce, gdy, na przykład, urządzenia w organizacji zawierają luki, które mogłyby zostać wyeliminowane przez te aktualizacje.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

- Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji

  Jeśli ta opcja jest włączona, informacje o lukach w oprogramowaniu innej firmy (w tym oprogramowaniu firmy Microsoft), wykrytych na zarządzanych urządzeniach, oraz o aktualizacjach oprogramowania, które eliminują luki innych firm (nie dotyczy oprogramowania firmy Microsoft) są wysyłane do Serwera administracyjnego.

  Wybranie tej opcji (**Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji)** zwiększy obciążenie sieci, obciążenie dysku Serwera administracyjnego oraz zużycie zasobów Agenta sieciowego.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

  Aby zarządzać aktualizacjami oprogramowania firmy Microsoft, użyj opcji **Szczegóły aktualizacji Windows Update**.

- Szczegóły rejestru sprzętu

  Agent sieciowy zainstalowany na urządzeniu wysyła informacje o sprzęcie urządzenia do Serwera administracyjnego. Możesz przejrzeć szczegóły sprzętu we właściwościach urządzenia.

- Szczegóły zainstalowanych aplikacji

Jeśli ta opcja jest włączona, informacje o aplikacjach zainstalowanych na urządzeniach klienckich są przesyłane do Serwera administracyjnego.

Domyślnie opcja ta jest włączona.

- **Dołącz informacje o poprawkach**

  Informacje o poprawkach aplikacji zainstalowanych na urządzeniach klienckich są wysyłane do Serwera administracyjnego. Włączenie tej opcji może zwiększyć obciążenie na Serwerze administracyjnym oraz DBMS, a także spowodować zwiększenie rozmiaru bazy danych.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

Okno Aktualizacje oprogramowania i luki

W sekcji **Aktualizacje oprogramowania i luki** możesz skonfigurować wyszukiwanie i rozsyłanie aktualizacji systemu Windows, a także włączyć skanowanie plików wykonywalnych w poszukiwaniu luk. Ustawienia w sekcji **Aktualizacje oprogramowania i luki** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows:

- **Użyj Serwera administracyjnego jako serwera WSUS**

  Jeśli ta opcja jest włączona, aktualizacje systemu Windows są pobierane na Serwer administracyjny. Serwer administracyjny dostarcza pobrane aktualizacje usłudze Windows Update na urządzeniach klienckich w trybie scentralizowanym przy użyciu Agentów sieciowych.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie używany do pobierania aktualizacji systemu Windows. W tym przypadku urządzenia klienckie same pobierają aktualizacje systemu Windows.

  Domyślnie opcja ta jest wyłączona.

- Pod sekcją **Zezwalaj użytkownikom na zarządzanie instalowaniem aktualizacji Windows Update** możesz ograniczyć aktualizacje Windows, które użytkownicy mogą ręcznie instalować na swoich urządzeniach przy użyciu Windows Update.

  Na urządzeniach działających pod kontrolą systemu Windows 10, jeśli usługa Windows Update już wykryła aktualizacje dla urządzenia, nowa opcja, którą wybierzesz w sekcji **Zezwalaj użytkownikom na zarządzanie instalowaniem aktualizacji Windows Update**, zostaną zastosowane dopiero po zainstalowaniu wykrytych aktualizacji.

  Wybierz element z listy rozwijalnej:

  - **Zezwalaj użytkownikom na instalację wszystkich dostępnych aktualizacji Windows Update**

    Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach.

    Wybierz tę opcję, jeśli nie chcesz uczestniczyć w instalacji aktualizacji.

    Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

- **Zezwalaj użytkownikom na instalację wszystkich zatwierdzonych aktualizacji Windows Update**

  Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach i które zostały zatwierdzone przez Ciebie.

  Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych zatwierdzonych aktualizacji.

  Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

- **Nie zezwalaj użytkownikom na instalowanie aktualizacji Windows Update**

  Użytkownicy nie mogą ręcznie zainstalować aktualizacji Microsoft Windows Update na swoich urządzeniach. Wszystkie stosowane aktualizacje są instalowane w sposób skonfigurowany przez Ciebie.

  Wybierz tę opcję, jeśli chcesz zarządzać instalacją aktualizacji w sposób scentralizowany.

  Na przykład, możesz chcieć zoptymalizować terminarz aktualizacji, aby sieć nie została przeciążona. Możesz skonfigurować terminarz aktualizacji po godzinach, aby nie przeszkadzały w pracy użytkowników.

- W grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** możesz wybrać tryb wyszukiwania aktualizacji:

  - **Aktywny**

    Jeśli ta opcja jest zaznaczona, Serwer administracyjny z pomocą Agenta sieciowego przesyła żądanie z Agenta Windows Update na urządzeniu klienckim do źródła uaktualnień: Serwery Windows Update lub WSUS. Następnie Agent sieciowy przesyła informacje z usługi Windows Update Agent do Serwera administracyjnego.

    Opcja zaczyna działać tylko wtedy, gdy zaznaczona jest opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

    Domyślnie opcja ta jest zaznaczona.

  - **Pasywny**

    Jeżeli ta opcja jest zaznaczona, Agent sieciowy co jakiś czas przesyła informacje od Serwera administracyjnego dotyczące aktualizacji pobranych przy ostatniej synchronizacji agenta usługi Windows Update ze źródłem uaktualnień. Jeśli nie zostanie przeprowadzona synchronizacja agenta usługi Windows Update ze źródłem uaktualnień, informacje o aktualizacjach Serwera administracyjnego będą przestarzałe.

    Wybierz tę opcję, jeśli chcesz uzyskać aktualizacje z pamięci podręcznej źródła uaktualnień.

  - **Wyłączono**

    Jeśli ta opcja jest zaznaczona, Serwer administracyjny nie żąda informacji dotyczących aktualizacji.

    Wybierz tę opcję, gdy, na przykład, chcesz najpierw przetestować aktualizacje na swoim lokalnym urządzeniu.

- Skanuj pliki wykonywalne w poszukiwaniu luk podczas ich uruchamiania

  Jeśli ta opcja jest włączona, pliki wykonywalne są skanowane w poszukiwaniu luk podczas ich uruchamiania.

  Domyślnie opcja ta jest włączona.

Zarządzanie ponownym uruchomieniem

W sekcji **Zarządzanie ponownym uruchamianiem** możesz określić działanie, jakie zostanie wykonane, jeśli system operacyjny musi być uruchomiony ponownie, gdy korzystasz, instalujesz lub dezinstalujesz aplikację. Ustawienia w sekcji **Zarządzanie ponownym uruchamianiem** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows:

- Nie uruchamiaj ponownie systemu operacyjnego

  System operacyjny nie zostanie uruchomiony ponownie.

- Jeżeli będzie to wymagane, automatycznie uruchom ponownie system operacyjny

  Jeśli jest to konieczne, system operacyjny zostanie automatycznie uruchomiony ponownie.

- Pytaj użytkownika o akcję

  Aplikacja pyta użytkownika o pozwolenie na ponowne uruchomienie systemu operacyjnego.

  Domyślnie opcja ta jest zaznaczona.

  - Ponawiaj pytanie co (min)

    Jeśli ta opcja jest włączona, aplikacja pyta użytkownika o pozwolenie na ponowne uruchomienie systemu operacyjnego z częstotliwością określoną w polu znajdującym się obok pola do zaznaczenia. Domyślnie częstotliwość wyświetlania pytania wynosi 5 minut.

    Jeśli ta opcja jest wyłączona, aplikacja nie ponawia pytania o pozwolenie na ponowne uruchomienie systemu.

    Domyślnie opcja ta jest włączona.

  - Wymuś restart po (min)

    Jeśli ta opcja jest włączona, po wyświetleniu pytania, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu czasu określonego w polu znajdującym się obok pola do zaznaczenia.

    Jeśli ta opcja jest wyłączona, aplikacja nie wymusza ponownego uruchomienia systemu.

    Domyślnie opcja ta jest włączona.

  - Czas oczekiwania przed wymuszeniem zamknięcia aplikacji dla zablokowanych sesji (min)

Wymuszone zamknięcie aplikacji ma miejsce, gdy urządzenie użytkownika jest zablokowane (automatycznie po określonym czasie nieaktywności lub ręcznie).

Jeśli ta opcja jest włączona, wymuszone zamknięcie aplikacji na zablokowanym urządzeniu odbywa się po minięciu czasu określonego w polu wejściowym.

Jeśli ta opcja jest wyłączona, aplikacje nie będą zamykane na zablokowanym urządzeniu.

Domyślnie opcja ta jest wyłączona.

Udostępnianie pulpitu Windows

W sekcji **Udostępnianie pulpitu Windows** możesz włączyć i skonfigurować audyt działań administratora wykonywanych na zdalnym urządzeniu podczas współdzielenia dostępu do pulpitu. Ustawienia w sekcji **Udostępnianie pulpitu Windows** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows:

- **Włącz audyt**

  Jeśli ta opcja jest włączona, audyt działań administratora na zdalnym urządzeniu jest włączony. Wpisy dotyczące działań administratora na zdalnym urządzeniu są zapisywane w:

  - Raporcie zdarzeń na zdalnym urządzeniu
  - W pliku z rozszerzeniem syslog, znajdującym się w folderze instalacyjnym Agenta sieciowego na zdalnym urządzeniu
  - W bazie danych zdarzeń programu Kaspersky Security Center

  Audyt działań administratora jest dostępny, gdy są spełnione następujące warunki:

  - Licencja Zarządzanie lukami i poprawkami jest w użyciu
  - Administrator posiada uprawnienie do włączania współdzielonego dostępu do pulpitu zdalnego urządzenia

  Jeśli ta opcja jest wyłączona, audyt działań administratora na zdalnym urządzeniu jest wyłączony.

  Domyślnie opcja ta jest wyłączona.

- **Maski plików, które będą monitorowane podczas odczytu**

  Lista zawiera maski plików. Jeśli audyt jest włączony, aplikacja monitoruje odczytywanie plików przez administratora, które odpowiadają maskom, i zapisuje informacje o odczycie plików. Lista jest dostępna, jeśli pole **Włącz audyt** jest zaznaczone. Możesz zmodyfikować maski plików i dodać nowe do listy. Każda nowa maska pliku powinna być określona na liście w nowym wierszu.

  Domyślnie określone są następujące maski plików:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Maski plików, które będą monitorowane podczas modyfikacji**

  Lista zawiera maski plików na zdalnym urządzeniu. Jeśli audyt jest włączony, aplikacja monitoruje zmiany wprowadzone przez administratora w plikach, które odpowiadają maskom, i zapisuje informacje o tych modyfikacjach. Lista jest dostępna, jeśli pole **Włącz audyt** jest zaznaczone. Możesz zmodyfikować maski plików i dodać nowe do listy. Każda nowa maska pliku powinna być określona na liście w nowym wierszu.

  Domyślnie określone są następujące maski plików:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Zarządzaj poprawkami i aktualizacjami

W sekcji **Zarządzaj poprawkami i aktualizacjami** możesz skonfigurować pobieranie i dystrybucję uaktualnień oraz instalację poprawek na zarządzanych urządzeniach:

- Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany

  Jeśli ta opcja jest włączona, poprawki Kaspersky ze stanem zatwierdzenia *Niezdefiniowane* będą automatycznie instalowane na zarządzanych urządzeniach natychmiast po pobraniu z serwerów aktualizacji.

  Jeśli ta opcja jest wyłączona, poprawki Kaspersky, które zostały pobrane i oznaczone jako *Niezdefiniowane*, zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzone*.

  Domyślnie opcja ta jest włączona.

- Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)

  Jeśli ta opcja jest włączona, tryb offline pobierania uaktualnień jest używany. Jeśli Serwer administracyjny pobierze uaktualnienia, powiadomi Agenta sieciowego (na urządzeniach, na których jest zainstalowany) o uaktualnieniach, które będą wymagane dla zarządzanych aplikacji. Jeśli Agent sieciowy otrzyma informacje o tych uaktualnieniach, pobierze odpowiednie pliki z Serwera administracyjnego z wyprzedzeniem. Przy pierwszym nawiązaniu połączenia z Agentem sieciowym, Serwer administracyjny inicjuje pobranie uaktualnień. Jeśli Agent sieciowy pobierze wszystkie uaktualnienia na urządzenie klienckie, staną się one dostępne dla aplikacji na tym urządzeniu.

  Jeśli zarządzana aplikacja na urządzeniu klienckim spróbuje uzyskać dostęp do Agenta sieciowego w celu uzyskania uaktualnień, Agent sieciowy sprawdzi, czy posiada wszystkie wymagane uaktualnienia. Jeśli uaktualnienia zostały pobrane z Serwera administracyjnego nie więcej niż 25 godzin przed zażądaniem ich przez zarządzaną aplikację, Agent sieciowy nie nawiąże połączenia z Serwerem administracyjnym, ale dostarczy zarządzanej aplikacji uaktualnienia z lokalnej pamięci podręcznej. Połączenie z Serwerem administracyjnym może nie zostać nawiązane, gdy Agent sieciowy dostarcza uaktualnienia aplikacji na urządzeniach klienckich, ale połączenie nie jest wymagane w celu przeprowadzenia aktualizacji.

  Jeśli ta opcja jest wyłączona, tryb offline pobierania uaktualnień nie jest używany. Uaktualnienia są rozsyłane zgodnie z terminarzem zadania pobierania uaktualnień.

  Domyślnie opcja ta jest włączona.

Łączność

Sekcja **Łączność** zawiera trzy zagnieżdżone podsekcje:

- **Sieć**
- **Profile połączenia** (tylko dla systemów Windows i macOS)
- **Terminarz połączeń**

W podsekcji **Sieć** możesz skonfigurować połączenie z Serwerem administracyjnym, włączyć korzystanie z portu UDP oraz określić jego numer. Dostępne są następujące opcje:

- W grupie ustawień **Połączenie z Serwerem administracyjnym** możesz skonfigurować połączenie z Serwerem administracyjnym oraz określić przedziału czasu dla synchronizacji pomiędzy urządzeniami klienckimi a Serwerem administracyjnym:
  - Kompresuj ruch sieciowy

Jeżeli ta opcja jest włączona, prędkość transferu danych przez Agenta sieciowego zostaje zwiększona poprzez zmniejszenie ilości przesyłanych informacji i tym samym zmniejszenie obciążenia Serwera administracyjnego.

Obciążenie procesora komputera klienckiego może się zwiększyć.

Domyślnie pole to jest zaznaczone.

- Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows

  Jeżeli ta opcja jest włączona, port UDP, niezbędny do pracy Agenta sieciowego, zostanie dodany do listy wykluczeń Zapory systemu Microsoft Windows.

  Domyślnie opcja ta jest włączona.

- Użyj SSL

  Jeśli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

  Domyślnie opcja ta jest włączona.

- Użyj bramy połączenia na punkcie dystrybucji (jeśli jest dostępny) w domyślnych ustawieniach połączenia

  Jeśli ta opcja jest włączona, brama połączenia na punkcie dystrybucji jest używana z ustawieniami określonymi we właściwościach grupy administracyjnej.

  Domyślnie opcja ta jest włączona.

- Użyj portu UDP

  Jeśli chcesz, żeby zarządzane urządzenia nawiązywały połączenie z serwerem KSN proxy poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

- Numer portu UDP

  W tym polu możesz wprowadzić numer portu UDP. Domyślny numer portu to 15000.

  Używany jest system dziesiętny.

  Jeżeli na urządzeniu klienckim zainstalowany jest system Windows XP Service Pack 2, wówczas wbudowana zapora sieciowa będzie blokowała port UDP o numerze 15000. Port ten należy otworzyć ręcznie.

- Użyj punktu dystrybucji do wymuszenia nawiązania połączenia z Serwerem administracyjnym

  Wybierz tę opcję, jeśli w oknie ustawień punktu dystrybucji zaznaczyłeś opcję **Użyj tego punktu dystrybucji jako serwera push**. W przeciwnym razie punkt dystrybucji nie będzie działał jako serwer push.

W podsekcji **Profile połączenia** możesz określić ustawienia lokalizacji sieciowej, skonfigurować profile połączenia dla Serwera administracyjnego, a także włączyć tryb użytkownika mobilnego, gdy Serwer administracyjny jest niedostępny. Ustawienia w sekcji **Profile połączenia** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows i macOS:

- **Ustawienia lokalizacji sieciowej**

  Ustawienia lokalizacji sieciowej definiują cechy sieci, do której podłączone jest urządzenie klienckie, i określają reguły przełączania Agenta sieciowego z jednego profilu połączenia Serwera administracyjnego do innego, gdy te cechy sieci zostaną zmienione.

- **Profile połączeń Serwera administracyjnego**

  W tej sekcji możesz dodawać i wyświetlać profile połączenia Agenta sieciowego z Serwerem administracyjnym. W tej sekcji możesz także utworzyć reguły przełączania Agenta sieciowego na inne Serwery administracyjne, gdy wystąpią następujące zdarzenia:

  - Gdy urządzenie klienckie zostanie podłączone do innej sieci lokalnej
  - Gdy zostanie zerwane połączenie między urządzeniem a siecią lokalną organizacji
  - Gdy adres bramy połączenia zostanie zmieniony lub adres serwera DNS zostanie zmodyfikowany

  Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

- **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny**

  Jeśli ta opcja jest włączona, w przypadku połączenia przez ten profil, aplikacje zainstalowane na urządzeniu klienckim będą używać profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie opcja ta jest wyłączona.

W podsekcji **Terminarz połączeń** możesz określić przedziały czasu, w trakcie których Agent sieciowy wysyła dane do Serwera administracyjnego:

- **Połącz, gdy jest to konieczne**

  Jeśli ta opcja jest zaznaczona, połączenie jest nawiązywane, gdy Agent sieciowy musi wysłać dane na Serwer administracyjny.

  Domyślnie opcja ta jest zaznaczona.

- **Połącz w określonych przedziałach czasu**

  Jeśli ta opcja jest zaznaczona, Agent sieciowy łączy się z Serwerem administracyjnym w określonym czasie. Możesz dodać kilka przedziałów czasu.

Punkty dystrybucji

Sekcja **Punkty dystrybucji** zawiera cztery zagnieżdżone podsekcje:

- **Przeszukiwanie sieci**
- **Ustawienia połączenia internetowego**
- **KSN Proxy**
- **Aktualizacje**

W podsekcji **Przeszukiwanie sieci** możesz skonfigurować automatyczne przeszukiwanie sieci. Można włączyć trzy typy przeszukiwania, czyli przeszukiwanie sieci, przeszukiwanie zakresu adresów IP i przeszukiwanie Active Directory:

- **Włącz przeszukiwanie sieci**

  Jeśli ta opcja jest włączona, Serwer administracyjny automatycznie przeszuka sieć zgodnie z terminarzem skonfigurowanym po kliknięciu odnośników **Ustaw terminarz szybkiego przeszukiwania** i **Ustaw terminarz pełnego przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie przeszukiwał sieci.

  Interwał wykrywania urządzeń dla Agenta sieciowego w wersjach przed 10.2 może zostać skonfigurowany w polach **Częstotliwość pobierania informacji z domen Windows (min)** i **Częstotliwość przeszukiwania sieci (min)**. Pola są dostępne, jeśli opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

- **Włącz przeszukiwanie zakresu IP**

  Jeśli opcja jest włączona, Serwer administracyjny automatycznie przeszuka zakresy IP zgodnie z terminarzem skonfigurowanym po kliknięciu odnośnika **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie przeszukiwał zakresów IP.

  Częstotliwość przeszukiwania zakresu IP dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

- **Użyj przeszukiwania Zeroconf (tylko na platformach Linux; ręcznie określone zakresy adresów IP zostaną zignorowane)**

  Jeśli ta opcja jest włączona, punkt dystrybucji automatycznie przeszukuje sieć za pomocą urządzeń IPv6, używając zero-configuration networking (zwany również *Zeroconf*). W takim przypadku włączone przeszukiwanie zakresu adresów IP jest ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć.

  W celu rozpoczęcia korzystania z Zeroconf, muszą być spełnione następujące warunki:

  - Punkt dystrybucji musi działać pod systemem Linux.
  - Musisz zainstalować narzędzie avahi-browse na punkcie dystrybucji.

  Jeśli ta opcja jest wyłączona, punkt dystrybucji nie przeszukuje sieci z urządzeniami IPv6.

  Domyślnie opcja ta jest wyłączona.

- **Włącz przeszukiwanie Active Directory**

Jeśli ta opcja jest włączona, Serwer administracyjny automatycznie przeszuka Active Directory zgodnie z terminarzem skonfigurowanym po kliknięciu odnośnika **Ustaw terminarz przeszukiwania**.

Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie przeszukiwał Active Directory.

Częstotliwość przeszukiwania Active Directory dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli ta opcja jest włączona.

Domyślnie opcja ta jest wyłączona.

W podsekcji **Ustawienia połączenia z Internetem** możesz określić ustawienia dostępu do Internetu:

- Użyj serwera proxy

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz skonfigurować połączenie z serwerem proxy.

  Domyślnie pole to nie jest zaznaczone.

- Adres serwera proxy

  Adres serwera proxy.

- Numer portu

  Numer portu używanego do nawiązywania połączenia.

- Pomiń serwer proxy dla adresów lokalnych

  Jeśli ta opcja jest włączona, żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

  Domyślnie opcja ta jest wyłączona.

- Uwierzytelnianie na serwerze proxy

  Jeśli to pole jest włączone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  Domyślnie, pole to jest wyłączone.

- Nazwa użytkownika

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy.

- Hasło

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

W podsekcji **KSN Proxy** możesz skonfigurować aplikację, aby używała punkt dystrybucji do przesyłania żądań KSN z zarządzanych urządzeń:

- **Włącz KSN Proxy po stronie punktu dystrybucji**

  Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

  Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky. Domyślnie, Oświadczenie KSN znajduje się w %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

  Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

- **Przesyłaj żądania KSN do Serwera administracyjnego**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dostęp do KSN Cloud/Private KSN bezpośrednio przez Internet**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub Private KSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub Private KSN.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej), nie może uzyskać bezpośredniego dostępu do Private KSN. Jeśli chcesz ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do prywatnej sieci KSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 12 (lub późniejszej), może uzyskać bezpośredni dostęp do Private KSN.

- **Port TCP**

  Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

- **Użyj portu UDP**

  Jeśli chcesz, żeby zarządzane urządzenia nawiązywały połączenie z serwerem KSN proxy poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

W podsekcji **Aktualizacje** możesz określić, czy Agent sieciowy powinien pobierać pliki diff poprzez włączenie lub wyłączenie opcji **Pobierz pliki diff** (domyślnie, ta opcja jest włączona).

Historia rewizji

W sekcji **Historia rewizji** możesz przejrzeć historię rewizji zasady Agenta sieciowego. Możesz porównać rewizje, przejrzeć rewizje i wykonać zaawansowane działania, takie jak zapisanie rewizji do pliku, wycofać rewizję oraz dodać i zmodyfikować opisy rewizji.

Porównanie funkcji w systemach operacyjnych Agenta sieciowego

Poniższa tabela pokazuje, jakich ustawień zasady Agenta sieciowego możesz użyć do skonfigurowania Agenta sieciowego z określonym systemem operacyjnym.

Ustawienia zasady Agenta sieciowego: porównanie według systemów operacyjnych

Sekcja Zasada	Windows	Mac	Linux
Ogólny	✓	✓	✓
Konfiguracja zdarzenia	✓	✓	✓
Ustawienia	✓	✓	✓ Dostępne są tylko opcje **Maksymalny rozmiar kolejki zdarzeń, w MB** oraz **Aplikacja może pobierać rozszerzone dane zasad na urządzenie**.
Repozytoria	✓	–	✓ Dostępne są tylko opcje **Szczegóły zainstalowanych aplikacji** i **Szczegóły rejestru sprzętu**.
Aktualizacje oprogramowania i luki	✓	–	–
Zarządzanie ponownym uruchamianiem	✓	–	–
Udostępnianie pulpitu Windows	✓	–	–
Zarządzaj poprawkami i aktualizacjami	✓	–	–
Łączność → Sieć	✓	✓	✓ Za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows**.
Łączność → Profile połączenia	✓	✓	–
Łączność → Terminarz połączeń	✓	✓	✓
Punkty dystrybucji → Przeszukiwanie sieci	✓	–	✓ Dostępna jest tylko sekcja **Przeszukiwanie zakresu IP**.
Punkty dystrybucji → Ustawienia połączenia internetowego	✓	✓	✓
Punkty dystrybucji → KSN Proxy	✓	–	–
Punkty dystrybucji → Aktualizacje	✓	–	–
Historia rewizji	✓	✓	✓

Zarządzanie kontami użytkowników

Ta sekcja dostarcza informacje o rolach i kontach użytkowników obsługiwanych przez aplikację. Sekcja zawiera także instrukcje dotyczące tworzenia kont i ról użytkowników Kaspersky Security Center.

Kaspersky Security Center umożliwia zarządzanie kontami użytkowników i grupami kont. Aplikacja obsługuje dwa typy kont:

- Konta pracowników firmy. Serwer administracyjny pobiera dane kont tych użytkowników podczas przeszukiwania sieci firmowej.
- Konta wewnętrznych użytkowników. Te konta są stosowane, gdy używane są wirtualne Serwery administracyjne. Konta użytkowników wewnętrznych są tworzone i używane tylko w obrębie Kaspersky Security Center.

Praca z kontami użytkowników

Kaspersky Security Center umożliwia zarządzanie kontami użytkowników i grupami kont. Aplikacja obsługuje dwa typy kont:

- Konta pracowników firmy. Serwer administracyjny pobiera dane kont tych użytkowników podczas przeszukiwania sieci firmowej.
- Konta wewnętrznych użytkowników. Te konta są stosowane, gdy używane są wirtualne Serwery administracyjne. Konta użytkowników wewnętrznych są tworzone i używane tylko w obrębie Kaspersky Security Center.

Wszystkie konta użytkowników można wyświetlić w folderze **Konta użytkowników** drzewa konsoli. Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

Na kontach użytkowników i grupach kont można wykonać następujące działania:

- Skonfigurować dla użytkowników uprawnienia dostępu do funkcji aplikacji przy użyciu ról.
- Wysłać wiadomości do użytkowników za pośrednictwem poczty elektronicznej i SMS-ów.
- Przeglądać listę urządzeń mobilnych użytkownika.
- Dostarczyć i zainstalować certyfikaty na urządzenia mobilne użytkownika.
- Wyświetl listę certyfikatów wydanych dla użytkownika.
- Wyłączyć weryfikację dwuetapową dla konta użytkownika.

Dodawanie konta użytkownika wewnętrznego

W celu dodania nowego konta użytkownika wewnętrznego do Kaspersky Security Center:

1. W drzewie konsoli otwórz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. W obszarze roboczym kliknij przycisk **Dodaj użytkownika**.

3. W otwartym oknie **Nowy użytkownik** określ ustawienia nowego konta użytkownika:

- Nazwa użytkownika ()

  > Należy ostrożnie wpisywać nazwę użytkownika. Nie będziesz mógł jej zmienić po zapisaniu zmian.

- **Opis**
- **Pełna nazwa**
- **Główny adres e-mail**
- **Główny numer telefonu**
- **Hasło** dla połączenia użytkownika z Kaspersky Security Center

  Hasło musi być zgodne z następującymi regułami:

  - Hasło musi zawierać od 8 do 16 znaków.
  - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
    - Wielkie litery (A-Z)
    - Małe litery (a-z)
    - Cyfry (0-9)
    - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

  Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

  > Liczba prób wprowadzenia hasła jest ograniczona. Domyślnie jest to 10 prób. Możesz zmienić dozwoloną liczbę prób wprowadzenia hasła, jak opisano to w sekcji „Zmienianie liczby dozwolonych prób wprowadzenia hasła".

  > Jeśli użytkownik wprowadzi nieprawidłowe hasło określoną liczbę razy, konto użytkownika zostanie zablokowane na jedną godzinę. Na liście kont użytkowników, ikona użytkownika () zablokowanego konta będzie ciemna (niedostępna). Możesz odblokować konto użytkownika tylko poprzez zmianę hasła.

- Jeśli to konieczne, zaznacz pole **Wyłącz konto**, aby zabronić użytkownikowi możliwość łączenia z aplikacją. Możesz wyłączyć konto, na przykład, jeśli chcesz je utworzyć teraz, ale aktywować później.
- Zaznacz pole **Poproś o hasło podczas modyfikowania ustawień konta**, jeśli chcesz włączyć dodatkową opcję ochrony konta użytkownika przed nieautoryzowaną modyfikacją. Jeżeli ta opcja jest włączona, modyfikowanie ustawień konta użytkownika wymaga autoryzacji użytkownika za pomocą uprawnienia Modyfikuj listy ACL obiektów obszaru funkcyjnego **Funkcje ogólne: Uprawnienia użytkownika**.

4. Kliknij **OK**.

Nowo utworzone konto użytkownika będzie wyświetlane w obszarze roboczym folderu **Konta użytkowników**.

Edytowanie konta użytkownika wewnętrznego

W celu edytowania konta użytkownika wewnętrznego w Kaspersky Security Center:

1. W drzewie konsoli otwórz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. W obszarze roboczym kliknij dwukrotnie konto użytkownika wewnętrznego, które chcesz edytować.

3. W otwartym oknie **Właściwości: <nazwa użytkownika>** zmień ustawienia konta użytkownika:

   - **Opis**
   - **Pełna nazwa**
   - **Główny adres e-mail**
   - **Główny numer telefonu**
   - **Hasło** dla połączenia użytkownika z Kaspersky Security Center

     Hasło musi być zgodne z następującymi regułami:

     - Hasło musi zawierać od 8 do 16 znaków.
     - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
       - Wielkie litery (A-Z)
       - Małe litery (a-z)
       - Cyfry (0-9)
       - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

     Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

     Liczba prób wprowadzenia hasła jest ograniczona. Domyślnie jest to 10 prób. Możesz zmienić dozwoloną liczbę prób wprowadzenia hasła, jak opisano to w sekcji „Zmienianie liczby dozwolonych prób wprowadzenia hasła”.

     Jeśli użytkownik wprowadzi nieprawidłowe hasło określoną liczbę razy, konto użytkownika zostanie zablokowane na jedną godzinę. Na liście kont użytkowników, ikona użytkownika () zablokowanego konta będzie ciemna (niedostępna). Możesz odblokować konto użytkownika tylko poprzez zmianę hasła.

   - Jeśli to konieczne, zaznacz pole **Wyłącz konto**, aby zabronić użytkownikowi możliwość łączenia z aplikacją. Możesz wyłączyć konto, na przykład, gdy pracownik opuści teren firmy.

- Wybierz opcję **Poproś o hasło podczas modyfikowania ustawień konta**, jeśli chcesz włączyć dodatkową opcję ochrony konta użytkownika przed nieautoryzowaną modyfikacją. Jeżeli ta opcja jest włączona, modyfikowanie ustawień konta użytkownika wymaga autoryzacji użytkownika za pomocą uprawnienia Modyfikuj listy ACL obiektów obszaru funkcyjnego **Funkcje ogólne: Uprawnienia użytkownika**.

4. Kliknij **OK**.

Edytowane konto użytkownika będzie wyświetlane w obszarze roboczym folderu **Konta użytkowników**.

Zmienianie liczby dozwolonych prób wprowadzenia hasła

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

Domyślnie, maksymalna liczba dozwolonych prób wprowadzenia hasła to 10. Możesz zmienić liczbę dozwolonych prób wprowadzenia hasła w sposób opisany w tej sekcji.

W celu zmiany liczny dozwolonych prób wprowadzenia hasła:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

2. Przejdź do gałęzi:

   - W systemach 32-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - W systemach 64-bitowych:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Jeśli brakuje wartości SrvSplPpcLogonAttempts, utwórz ją. Typ wartości to DWORD.
   Domyślnie, po zainstalowaniu Kaspersky Security Center, ta wartość nie zostaje utworzona.

4. Określ żądaną liczbę prób w wartości SrvSplPpcLogonAttempts.

5. Kliknij **OK**, aby zachować zmiany.

6. Uruchom ponownie usługę Serwera administracyjnego.

Maksymalna liczba dozwolonych prób wprowadzenia hasła zostanie zmieniona.

Konfigurowanie sprawdzania unikatowości nazwy użytkownika wewnętrznego

Możesz skonfigurować sprawdzanie unikatowości nazwy użytkownika wewnętrznego Kaspersky Security Center podczas dodawania nazwy do aplikacji. Sprawdzanie unikatowości nazwy użytkownika wewnętrznego może zostać przeprowadzone tylko na wirtualnym Serwerze administracyjnym lub na głównym Serwerze administracyjnym, dla którego będzie tworzone konto użytkownika, lub na wszystkich wirtualnych Serwerach administracyjnych i na głównym Serwerze administracyjnym. Domyślnie unikatowość nazwy użytkownika wewnętrznego jest sprawdzana na wszystkich wirtualnych Serwerach administracyjnych i na głównym Serwerze administracyjnym.

W celu sprawdzenia unikatowości nazwy użytkownika wewnętrznego na wirtualnym Serwerze administracyjnym lub na głównym Serwerze administracyjnym:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

2. Przejdź do gałęzi:

   - W systemach 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

   - W systemach 64-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Dla klucza LP_InterUserUniqVsScope (DWORD) ustaw wartość 00000001.

   0 jest domyślną wartością określoną dla tego klucza.

4. Uruchom ponownie usługę Serwera administracyjnego.

   Unikatowość nazwy będzie sprawdzana na wirtualnym Serwerze administracyjnym, na którym został utworzony użytkownik wewnętrzny, lub na głównym Serwerze administracyjnym, jeśli użytkownik wewnętrzny został utworzony na głównym Serwerze administracyjnym.

W celu sprawdzenia unikatowości nazwy użytkownika wewnętrznego na wszystkich wirtualnych Serwerach administracyjnych lub na głównym Serwerze administracyjnym:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

2. Przejdź do gałęzi:

   - Dla systemu 64-bitowego:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

   - Dla systemu 32-bitowego:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Dla klucza LP_InterUserUniqVsScope (DWORD) ustaw wartość 00000000.

   0 jest domyślną wartością określoną dla tego klucza.

4. Uruchom ponownie usługę Serwera administracyjnego.

   Unikatowość nazwy będzie sprawdzana na wszystkich wirtualnych Serwerach administracyjnych i na głównym Serwerze administracyjnym.

Dodawanie grupy bezpieczeństwa

Możesz dodawać grupy bezpieczeństwa (grupy użytkowników), przeprowadzać elastyczną konfigurację dostępu grup i grupy bezpieczeństwa do różnych funkcji aplikacji. Grupom bezpieczeństwa można przypisać nazwy, które odpowiadają ich przeznaczeniu. Na przykład, nazwa może odpowiadać miejscu w biurze, w którym znajdują się użytkownicy, lub nazwie jednostki organizacyjnej firmy, do której należą użytkownicy.

Jeden użytkownik może należeć do kilku grup bezpieczeństwa. Konto użytkownika zarządzane przez wirtualny Serwer administracyjny może należeć tylko do grup bezpieczeństwa tego Serwera wirtualnego i może posiadać uprawnienia dostępu tylko w obrębie tego Serwera wirtualnego.

W celu dodania grupy bezpieczeństwa:

1. Z drzewa konsoli wybierz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Kliknij przycisk **Dodaj grupę zabezpieczeń**.

   Zostanie otwarte okno **Dodaj grupę zabezpieczeń**.

3. W oknie **Dodaj grupę zabezpieczeń**, w sekcji **Ogólny** określ nazwę grupy.

   Nazwa grupy nie może zawierać więcej niż 255 znaków oraz znaków specjalnych, takich jak: *, <, >, ?, \, :, |. Nazwa grupy musi być unikatowa.

   Opis grupy można wpisać w polu **Opis**. Uzupełnienie pola **Opis** nie jest obowiązkowe.

4. Kliknij **OK**.

Dodana grupa bezpieczeństwa pojawi się w folderze **Konta użytkowników** drzewa konsoli. Możesz dodawać użytkowników do nowo utworzonej grupy.

Dodawanie użytkownika do grupy

W celu dodania użytkownika do grupy:

1. Z drzewa konsoli wybierz folder **Konta użytkowników**.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Na liście grup i kont użytkowników wskaż grupę, do której chcesz dodać użytkownika.

3. W oknie właściwości grupy wybierz sekcję **Użytkownicy grupy** i kliknij przycisk **Dodaj**.

   Zostanie otwarte okno z listą użytkowników.

4. Na liście wskaż użytkownika, którego chcesz włączyć do grupy.

5. Kliknij **OK**.

Użytkownik zostaje dodany do grupy i wyświetlony na liście użytkowników grupy.

Konfigurowanie praw dostępu do funkcji aplikacji. Kontrola dostępu oparta o rolę

Kaspersky Security Center oferuje możliwości dla dostępu opartego na roli do funkcji Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky.

Możesz skonfigurować uprawnienia dostępu do funkcji aplikacji dla użytkowników Kaspersky Security Center w jeden z następujących sposobów:

- Konfigurując uprawnienia dla każdego użytkownika lub grupy użytkowników indywidualnie.
- Tworząc standardowe role użytkownika z predefiniowanym zestawem uprawnień i przypisując te role do użytkowników w zależności od ich zakresu obowiązków.

Rola użytkownika (zwana również rolą) jest predefiniowanym zestawem uprawnień dostępu do funkcji Kaspersky Security Center lub zarządzanych aplikacji firmy Kaspersky. Rola może zostać przydzielona użytkownikowi lub grupie użytkowników.

Stosowanie ról użytkownika jest przeznaczone do uproszczenia i skrócenia rutynowych procedur konfigurowania uprawnień dostępu użytkowników do funkcji aplikacji. Uprawnienia dostępu w obrębie roli są konfigurowane zgodnie ze 'standardowymi' zadaniami i zakresem obowiązków użytkowników.

Rolom użytkownika można przypisać nazwy, które odpowiadają ich przeznaczeniu. Możesz utworzyć nieograniczoną liczbę ról.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role i samodzielnie skonfigurować wymagane uprawnienia.

Prawa dostępu do funkcji aplikacji

Poniższa tabela przedstawia funkcje Kaspersky Security Center wraz z prawami dostępu do zarządzania powiązanymi zadaniami, raportami, ustawieniami i wykonywania powiązanych działań użytkownika.

Aby wykonać czynności użytkownika wymienione w tabeli, użytkownik musi mieć określone uprawnienia obok akcji.

Prawa do **odczytu**, **wpisywania** i **wykonywania** mają zastosowanie do każdego zadania, raportu lub ustawienia. Oprócz tych praw użytkownik musi mieć uprawnienie **Wykonaj operacje na wyborach urządzeń**, aby zarządzać zadaniami, raportami lub ustawieniami wyborów urządzeń.

Wszystkie zadania, raporty, ustawienia i pakiety instalacyjne, których brakuje w tabeli, należą do obszaru funkcjonalnego **Funkcje ogólne: Podstawowa funkcjonalność**.

Prawa dostępu do funkcji aplikacji

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport
Funkcje ogólne: **Zarządzanie grupami administracyjnymi**	**Wpisz**	• Dodaj urządzenie do grupy administracyjnej: **Wpisz** • Usuń urządzenie z grupy administracyjnej: **Wpisz** • Dodaj grupę administracyjną do innej grupy administracyjnej: **Wpisz** • Usuń grupę administracyjną z innej grupy	Brak	Brak

		administracyjnej: **Wpisz**		
Funkcje ogólne: **Uzyskuj dostęp do obiektów bez względu na ich listy ACL**	**Odczyt**	Uzyskaj dostęp do odczytu do wszystkich obiektów: **Odczyt**	Brak	Brak
Cechy ogólne: Podstawowa funkcjonalność	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Reguły przenoszenia urządzeń (tworzenie, modyfikowanie lub usuwanie) dla Serwera wirtualnego: **Wpisz**, **Wykonuj** operacje na wybranych urządzeniach • Uzyskaj niestandardowy certyfikat protokołu Mobile (LWNGT): **Odczytaj** • Ustaw certyfikat niestandardowy protokołu Mobile (LWNGT): **Zapisz** • Uzyskaj listę sieci zdefiniowaną przez NLA: **Odczytaj** • Dodaj, zmodyfikuj lub usuń listę sieci zdefiniowaną przez NLA: **Wpisz** • Wyświetl listę kontroli dostępu grup: **Odczytaj** • Wyświetl dziennik zdarzeń aplikacji Kaspersky: **Odczytaj**	• „Pobierz aktualizacje do repozytorium serwera administracyjnego” • „Dostarczaj raporty” • „Roześlij pakiet instalacyjny” • „Zdalnie zainstaluj aplikację na podrzędnych Serwerach administracyjnych”	• „Raport o sta ochrony” • „Raport o zagrożeniach” • „Raport o najbardziej zainfekowany urządzeniach” • „Raport o sta antywirusowy baz danych” • „Raport o błędach” • „Raport o ata sieciowych” • „Raport podsumowuja na temat zainstalowany aplikacji chroniących system poczt • „Raport podsumowuja na temat zainstalowany aplikacji ochro obwodowej” • „Raport podsumowuja na temat typo zainstalowany aplikacji” • „Raport o użytkownikac zainfekowany urządzeń” • „Raport incydentów”

				• „Raport wyda • „Raport o aktywności punktów dystrybucji" • „Raport o podrzędnych Serwerach administracyj • „Raport zdarz Kontroli urząc • „Raport o luka • „Raport o zabronionych aplikacjach" • „Raport Kontr sieci" • „Raport o sta szyfrowania zarządzanych urządzeń" • „Raport o sta szyfrowania urządzeń pam masowej" • „Raport o błę podczas szyfrowania plików" • „Raport o zablokowanyr dostępie do zaszyfrowany plików" • „Raport o uprawnieniacl dostępu do zaszyfrowany urządzeń" • „Raport o efektywnych uprawnieniacl użytkowników • „Raport dotyc uprawnień"

Funkcje ogólne: **Obiekty usunięte**	• **Odczyt** • **Wpisz**	• Wyświetl usunięte obiekty w Koszu: **Odczytaj** • Usuń obiekty z Kosza: **Wpisz**	Brak	Brak
Funkcje ogólne: **Przetwarzanie zdarzeń**	• **Usuń zdarzenia** • **Edytuj ustawienia powiadomień o zdarzeniach** • **Edytuj ustawienia rejestrowania zdarzeń** • **Wpisz**	• Zmień ustawienia rejestracji zdarzeń: **Edytuj ustawienia rejestrowania zdarzeń** • Zmień ustawienia powiadomień o zdarzeniach: **Edytuj ustawienia powiadomień o zdarzeniach** • Usuń zdarzenia: **Usuń zdarzenia**	Brak	Brak
Funkcje ogólne: **Operacje na Serwerze administracyjnym**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Modyfikuj listy ACL obiektów** • **Wykonaj operacje na wyborach urządzeń**	• Określ porty Serwera administracyjnego dla połączenia agenta sieciowego: **Wpisz** • Określ porty Serwera proxy aktywacji uruchomionego na serwerze administracyjnym Serwer administracyjny: **Wpisz** • Określ porty serwera proxy aktywacji dla urządzeń przenośnych	• „Tworzenie kopii zapasowych danych Serwera administracyjnego” • „Konserwacja baz danych”	Brak

		uruchomionych na Serwerze administracyjnym: **Wpisz** • Określ porty serwera sieciowego do dystrybucji samodzielnych pakietów: **Wpisz** • Określ porty serwera sieciowego do dystrybucji profili MDM: **Wpisz** • Określ porty SSL Serwera administracyjnego do połączenia przez Kaspersky Security Center Web Console: **Wpisz** • Określ porty serwera administracyjnego Serwer administracyjny dla połączenia mobilnego: **Wpisz** • Zmienianie maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego: **Wpisz** • Określ maksymalną liczbę zdarzeń, które mogą być wysłane przez Serwer administracyjny: **Wpisz** • Określ przedział czasu, w którym zdarzenia mogą być wysyłane przez Serwer administracyjny: **Wpisz**	

Funkcje ogólne: **Wdrażanie oprogramowania Kaspersky**	• **Zarządzaj poprawkami Kaspersky** • **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	Zaakceptuj lub odrzuć instalację poprawki: **Zarządzaj poprawkami Kaspersky**	Brak	• „Raport dotyc użycia klucza licencyjnego p wirtualny serv administracyjn • „Raport o wersjach oprogramowa Kaspersky” • „Raport o niekompatybi aplikacjach” • „Raport o wersjach aktualizacji modułu oprogramowa Kaspersky” • „Raport wdraż ochrony”
Cechy ogólne: **Zarządzanie kluczami**	• **Eksportuj plik klucza** • **Wpisz**	• Eksportuj plik klucza: **Eksportuj plik klucza** • Zmodyfikuj ustawienia klucza licencyjnego Serwera administracyjnego: **Wpisz**	Brak	Brak
Funkcje ogólne: **Wymuszone zarządzanie raportami**	• **Odczyt** • **Wpisz**	• Twórz raporty niezależnie od ich list ACL: **Zapisz** • Wykonywanie raportów niezależnie od ich list ACL: **Odczytaj**	Brak	Brak
Funkcje ogólne: **Hierarchia serwerów administracyjnych**	**Skonfiguruj hierarchię Serwerów administracyjnych**	Zarejestruj, zaktualizuj lub usuń podrzędne Serwery administracyjne: **Skonfiguruj hierarchię Serwerów administracyjnych**	Brak	Brak
Cechy ogólne:	**Modyfikuj listy ACL**	• Zmień właściwości	Brak	Brak

Uprawnienia użytkownika	**obiektów**	Zabezpieczenia dowolnego obiektu: **Modyfikuj listy ACL obiektów** • Zarządzaj rolami użytkowników: **Modyfikuj listy ACL obiektów** • Zarządzaj użytkownikami wewnętrznymi: **Modyfikuj listy ACL obiektów** • Zarządzaj grupami zabezpieczeń: **Modyfikuj listy ACL obiektów** • Zarządzaj aliasami: **Modyfikuj listy ACL obiektów**		
Funkcje ogólne: **Wirtualne serwery administracyjne**	• **Zarządzaj wirtualnym serwerem administracyjnym Serwery administracyjne** • **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Pobierz listę wirtualnych serwerów administracyjnych Serwery administracyjne: **Odczytaj** • Uzyskaj informacje na temat wirtualnego Serwera administracyjnego: **Odczytaj** • Utwórz, zaktualizuj lub usuń wirtualny Serwer administracyjny: **Zarządzaj wirtualnymi serwerami administracyjnymi** • Przenieś wirtualny Serwer administracyjny do innej grupy: **Zarządzaj wirtualnymi serwerami administracyjnymi**	Brak	„Raport o wynika instalacji aktualiz oprogramowania trzecich”

		• Ustaw uprawnienia do administracyjnego Serwera wirtualnego: **Zarządzaj wirtualnymi serwerami administracyjnymi**		
Funkcje ogólne: **Zarządzanie kluczami szyfrowania**	• **Odczyt** • **Wpisz**	• Eksportuj klucze szyfrowania: **Odczyt** • Zaimportuj klucze szyfrowania: **Wpisz**	Brak	Brak
Zarządzanie urządzeniami mobilnymi: **Ogólne**	• **Podłączanie nowych urządzeń** • **Wysyłaj tylko polecenia informacyjne na urządzenia mobilne** • **Wysyłanie poleceń na urządzenia mobilne** • **Zarządzaj certyfikatami** • **Odczyt** • **Wpisz**	• Uzyskaj dane przywracania Usługi zarządzania kluczami: **Odczytaj** • Usuń certyfikaty użytkownika: **Zarządzaj certyfikatami** • Uzyskaj część publiczną certyfikatu użytkownika: **Odczytaj** • Sprawdź, czy infrastruktura klucza publicznego jest włączona: **Odczytaj** • Sprawdź konto infrastruktury klucza publicznego: **Odczytaj** • Uzyskaj szablony infrastruktury klucza publicznego: **Odczytaj** • Uzyskaj szablony infrastruktury klucza publicznego za pomocą	Brak	Brak

		certyfikatu rozszerzonego użycia klucza: **Odczytaj** • Sprawdź, czy certyfikat infrastruktury klucza publicznego został odwołany: **Odczytaj** • Zaktualizuj ustawienia wydawania certyfikatów użytkownika: **Zarządzaj certyfikatami** • Uzyskaj ustawienia wydawania certyfikatu użytkownika: **Odczytaj** • Pobierz pakiety według nazwy i wersji aplikacji: **Odczytaj** • Ustaw lub anuluj certyfikat użytkownika: **Zarządzaj certyfikatami** • Odnów certyfikat użytkownika: **Zarządzaj certyfikatami** • Ustaw tag certyfikatu użytkownika: **Zarządzaj certyfikatami** • Uruchom generację pakietu instalacyjnego MDM; anuluj generowanie pakietu instalacyjnego MDM: **Podłącz nowe urządzenia**		

Zarządzanie systemem: **Łączność**	• **Rozpocznij sesje RDP** • **Połącz się z istniejącymi sesjami RDP** • **Rozpocznij tunelowanie** • **Zapisz pliki z urządzeń na stacji roboczej administratora** • **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Utwórz sesję udostępniania pulpitu: **Prawo do tworzenia sesji udostępniania pulpitu** • Utwórz sesję RDP: **Połącz się z istniejącymi sesjami RDP** • Utwórz tunel: **Zainicjuj tunelowanie** • Zapisz listę sieci partnerskiej: **Zapisz pliki z urządzeń na stacji roboczej administratora**	Brak	„Raport o użytkownikach urządzenia”
Zarządzanie systemem: **Inwentaryzacja sprzętu**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Pobierz lub wyeksportuj obiekt spisu sprzętu: **Odczytaj** • Dodaj, ustaw lub usuń obiekt spisu sprzętu: **Zapisz**	Brak	• „Raport rejest sprzętu” • „Raport o zmianach konfiguracji” • „Raport o sprzęcie”
Zarządzanie systemem: **Kontrola dostępu do sieci**	• **Odczyt** • **Wpisz**	• Wyświetl ustawienia CISCO: **Odczytaj** • Zmień ustawienia CISCO: **Zapisz**	Brak	Brak
Zarządzanie systemem: **Wdrażanie systemu operacyjnego**	• **Instalowanie serwerów PXE** • **Odczyt** • **Wpisz** • **Wykonaj**	• Zainstaluj serwer PXE: **Instalowanie serwerów PXE** • Wyświetl listę serwerów PXE: **Odczytaj** • Rozpocznij lub zatrzymaj proces	„Utwórz pakiet instalacyjny na podstawie obrazu systemu operacyjnego urządzenia odniesienia”	Brak

	• **Wykonaj operacje na wyborach urządzeń**	instalacji na klientach PXE: **Wykonaj** • Zarządzaj sterownikami dla WinPE i obrazów systemu operacyjnego: **Wpisz**		
Zarządzanie systemem: **zarządzanie lukami i poprawkami**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Wyświetl właściwości poprawki trzeciej firmy: **Odczytaj** • Zmień właściwości poprawki trzeciej firmy: **Wpisz**	• „Wykonać synchronizację Windows Update" • „Instalacja aktualizacji Windows Update" • „Napraw luki" • „Zainstaluj wymagane aktualizacje i napraw luki"	„Raport o aktualizacjach oprogramowania
Zarządzanie systemem: **Zdalna instalacja**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Przejrzyj właściwości pakietu instalacyjnego Zarządzanie lukami i poprawkami innych firm: **Odczytaj** • Zmień właściwości pakietu instalacyjnego Zarządzanie lukami i poprawkami innych firm: **Wpisz**	Brak	Brak
Zarządzanie systemem: **Inwentaryzacja oprogramowania**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	Brak	Brak	• „Raport o zainstalowany aplikacjach" • „Raport o rejestrze aplik • „Raport o sta grup licencjonowar aplikacji"

				• „Raport dotyc kluczy licencyjnych oprogramowa innych firm”

Informacje o rolach użytkowników

Role użytkowników przypisane do użytkowników Kaspersky Security Center zapewniają im zestawy praw dostępu do funkcji aplikacji.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role i samodzielnie skonfigurować wymagane uprawnienia. Niektóre z predefiniowanych ról użytkowników dostępnych w Kaspersky Security Center mogą być powiązane z określonymi stanowiskami pracy, na przykład **Audytor**, **Specjalista ds. zabezpieczeń**, **Opiekun** (te role są obecne w Kaspersky Security Center od wersji 11). Prawa dostępu do tych ról są wstępnie skonfigurowane zgodnie ze standardowymi zadaniami i zakresem obowiązków powiązanych stanowisk. Poniższa tabela pokazuje jak role mogą zostać powiązane z określonymi stanowiskami pracy:

Przykłady ról dla określonych stanowisk pracy

Rola	Komentarz
Audytor	Zezwala na wszystkie działania na wszystkich typach raportów, na wszystkie działania przeglądania, w tym przeglądanie usuniętych obiektów (nadaje uprawnienia **Odczyt** i **Zapisz** w obszarze **Usunięte obiekty**). Nie zezwala na pozostałe działania. Tę rolę można przypisać do osoby, która przeprowadza audyt w Twojej organizacji.
Opiekun	Zezwala na wszystkie działania przeglądania, ale nie zezwala na pozostałe działania. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Specjalista ds. zabezpieczeń	Zezwala na wszystkie działania przeglądania, zezwala na zarządzanie raportami; przydziela ograniczone uprawnienia w obszarze **Zarządzanie systemami**: **Łączność**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.

Poniższa tabela przedstawia prawa dostępu przypisane do każdej predefiniowanej roli użytkownika.

Prawa dostępu do predefiniowanych ról użytkowników

Rola	Opis

Administrator serwera administracyjnego	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Przetwarzanie zdarzeń**
	  • **Hierarchia Serwerów administracyjnych**
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie systemami**:
	  • **Łączność**

	• **Inwentaryzacja sprzętu** • **Inwentaryzacja oprogramowania** Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.

Operator serwera administracyjnego	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie systemami**:
	  • **Łączność**
	  • **Inwentaryzacja sprzętu**
	  • **Inwentaryzacja oprogramowania**

Audytor	Zezwala na wszystkie operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Usunięte obiekty** • **Wymuszone zarządzanie raportami** Tę rolę można przypisać do osoby, która przeprowadza audyt w Twojej organizacji.

Administrator instalacji	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Zdalna instalacja oprogramowania Kaspersky**
	  • **Zarządzanie kluczami licencyjnymi**
	• **Zarządzanie systemami**:
	  • **Nazwa systemu operacyjnego**
	  • **Zarządzanie lukami i poprawkami**
	  • **Instalacja zdalna**
	  • **Inwentaryzacja oprogramowania**
	Przyznaje uprawnienia do **odczytu** i **wykonywania** w obszarze funkcjonalnym **Funkcje ogólne: Wirtualne serwery administracyjne**.

Operator	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących

instalacji	obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Zdalna instalacja oprogramowania Kaspersky** (zapewnia również **Zarządzanie poprawkami Kaspersky** bezpośrednio w tym obszarze)
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie systemami**:
	  • **Nazwa systemu operacyjnego**
	  • **Zarządzanie lukami i poprawkami**
	  • **Instalacja zdalna**
	  • **Inwentaryzacja oprogramowania**

Administrator Kaspersky Endpoint Security	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.
Operator Kaspersky Endpoint Security	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
Główny administrator	Zezwala na wszystkie operacje w obszarach funkcjonalnych, z *wyjątkiem* następujących obszarów w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami** Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.

Główny operator	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) we wszystkich następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Usunięte obiekty**
	  • **Operacje na Serwerze administracyjnym**
	  • **Wdrażanie oprogramowania Kaspersky**

	• **Wirtualne Serwery administracyjne** • **Zarządzanie urządzeniami mobilnymi: ogólne** • **Zarządzanie systemem**, w tym wszystkie funkcje • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
Administrator zarządzania urządzeniami mobilnymi	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • **Zarządzanie urządzeniami mobilnymi: ogólne**
Operator zarządzania urządzeniami mobilnymi	Przyznaje uprawnienia **Odczyt** i **Wykonywanie** w obszarze funkcjonalnym **Funkcje ogólne**: **Podstawowa funkcjonalność**. Przyznaje uprawnienia **odczytu** i **wysyłania** informacji poleceń na urządzenia mobilne w obszarach funkcjonalnych **Zarządzania urządzeniami mobilnymi**: **Ogólne**.
Specjalista ds. zabezpieczeń	Zezwala na następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami** Przyznaje uprawnienia **Odczytu**, **Wpisania**, **Wykonywania**, **Zapisywania** plików z urządzeń na stacji roboczej administratora i **wykonywania działań dla wyborów urządzeń w obszarze funkcjonalnym Zarządzanie systemami: Łączność**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.
Użytkownik portalu Self Service Portal	Zezwala na wszystkie operacje w obszarze funkcjonalnym **Zarządzanie urządzeniami mobilnymi: Self Service Portal**. Ta funkcja nie jest obsługiwana w Kaspersky Security Center 11 i nowszej wersji.
Opiekun	Przyznaje prawo do **Odczytu** w obszarach funkcjonalnych **Funkcje ogólne**: **Dostęp do obiektów, niezależnie od ich list ACL** i **Funkcje ogólne**: **Wymuszone zarządzanie raportami**. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Administrator zarządzania lukami i poprawkami	Zezwala na wszystkie operacje w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje).
Operator zarządzania lukami i poprawkami	Przyznaje uprawnienia **Odczyt** i **Wykonywanie** (w stosownych przypadkach) w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje).

Dodawanie roli użytkownika

W celu dodania roli użytkownika:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

3. W oknie właściwości Serwera administracyjnego, na panelu **Sekcje** wybierz **Role użytkownika** i kliknij przycisk **Dodaj**.

   Sekcja **Role użytkownika** jest dostępna, jeśli włączona jest opcja **Wyświetl sekcje ustawień zabezpieczeń**.

4. W oknie właściwości **Nowa rola** skonfiguruj rolę:

   - Na panelu **Sekcje** wybierz **Ogólny** i określ nazwę roli.

     Nazwa roli nie może zawierać więcej niż 100 znaków.

   - Wybierz sekcję **Uprawnienia** i skonfiguruj zestaw uprawnień, zaznaczając pola **Zezwól** i **Odmów** obok funkcji aplikacji.

   Jeśli pracujesz na głównym Serwerze administracyjnym, możesz włączyć opcję **Przekaż listę ról do podrzędnych Serwerów administracyjnych**.

5. Kliknij **OK**.

Rola została dodana.

Role użytkownika utworzone dla Serwera administracyjnego są wyświetlane w oknie właściwości Serwera administracyjnego, w sekcji **Role użytkownika**. Możesz zmodyfikować i usunąć role użytkownika, a także przypisać role do grup użytkowników lub wybranych użytkowników.

Przypisywanie roli do użytkownika lub grupy użytkowników

W celu przypisania roli do użytkownika lub grupy użytkowników:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

3. W oknie właściwości Serwera administracyjnego wybierz sekcję **Zabezpieczenia**.

   Sekcja **Zabezpieczenia** jest dostępna, jeśli w oknie ustawień interfejsu dostępne jest pole **Wyświetl sekcje ustawień zabezpieczeń**.

4. W polu **Nazwy grup lub użytkowników** wybierz użytkownika lub grupę użytkowników, do których mają zostać przypisane role.

   Jeśli pole nie zawiera użytkownika lub grupy, możesz je dodać, klikając przycisk **Dodaj**.

   Jeśli dodajesz użytkownika poprzez kliknięcie przycisku **Dodaj**, możesz wybrać typ autoryzacji użytkownika (Microsoft Windows lub Kaspersky Security Center). Autoryzacja Kaspersky Security Center jest używana do wybierania kont wewnętrznych użytkowników, które są używane do pracy z wirtualnymi Serwerami administracyjnymi.

5. Wybierz zakładkę **Role** i kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Role użytkownika**. To okno wyświetla utworzone role użytkownika.

6. W oknie **Role użytkownika** wybierz rolę dla grupy użytkowników.

7. Kliknij **OK**.

Rola z zestawem uprawnień do pracy z Serwerem administracyjnym zostanie przypisana do użytkownika lub grupy. Przypisane role są wyświetlane na zakładce **Role**, w sekcji **Zabezpieczenia** okna właściwości Serwera administracyjnego.

Przydzielanie uprawnień użytkownikom i grupom

Użytkownikom i grupom możesz nadać uprawnienia do używania różnych funkcji Serwera administracyjnego i programów Kaspersky, dla których posiadasz wtyczki zarządzające, na przykład, Kaspersky Endpoint Security for Windows.

W celu przypisania uprawnień do użytkownika lub grupy użytkowników:

1. W drzewie konsoli wykonaj jedną z następujących czynności:

   - Rozwiń węzeł **Serwer administracyjny** i wybierz podfolder z nazwą żądanego Serwera administracyjnego.
   - Wybierz grupę administracyjną.

2. Z menu kontekstowego Serwera administracyjnego lub grupy administracyjnej wybierz **Właściwości**.

3. W otwartym oknie właściwości Serwera administracyjnego (lub oknie właściwości grupy administracyjnej), w lewym panelu **Sekcje** wybierz **Zabezpieczenia**.

   Sekcja **Zabezpieczenia** jest dostępna, jeśli w oknie ustawień interfejsu dostępne jest pole **Wyświetl sekcje ustawień zabezpieczeń**.

4. W sekcji **Zabezpieczenia**, na liście **Nazwy grup lub użytkowników** wybierz użytkownika lub grupę.

5. Na liście uprawnień w dolnej części obszaru roboczego, na zakładce **Uprawnienia** skonfiguruj zestaw uprawnień dla użytkownika lub grupy:

   a. Kliknij znaki plusa (+), aby rozwinąć węzły na liście i uzyskać dostęp do uprawnień.

   b. Zaznacz pola **Zezwól** i **Odmów** obok żądanych uprawnień.

      Przykład 1: Rozwiń węzeł **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** lub węzeł **Usunięte obiekty** i wybierz **Odczyt**.

      Przykład 2: Rozwiń węzeł **Podstawowa funkcjonalność** i wybierz **Zapis**.

6. Jeśli skonfigurowałeś zestaw uprawnień, kliknij **Zastosuj**.

Zestaw uprawnień dla użytkownika lub grupy użytkowników zostanie skonfigurowany.

Uprawnienia Serwera administracyjnego (lub grupy administracyjnej) są podzielone na następujące obszary:

- Funkcje ogólne:
  - Zarządzanie grupami administracyjnymi (tylko dla Kaspersky Security Center 11 lub nowszej wersji)

    - Uzyskuj dostęp do obiektów bez względu na ich listy ACL (tylko dla Kaspersky Security Center 11 lub nowszej wersji)
    - Podstawowa funkcjonalność
    - Usunięte obiekty (tylko dla Kaspersky Security Center 11 lub nowszej wersji)
    - Przetwarzanie zdarzeń
    - Operacje na Serwerze administracyjnym (tylko w oknie właściwości Serwera administracyjnego)
    - Zdalna instalacja aplikacji Kaspersky
    - Zarządzanie kluczami licencyjnymi
    - Wymuszone zarządzanie raportami (tylko dla Kaspersky Security Center 11 lub nowszej wersji)
    - Hierarchia Serwerów
    - Uprawnienia użytkownika
    - Wirtualne Serwery administracyjne
- Zarządzanie urządzeniami mobilnymi:
    - Ogólne
- Zarządzanie poprawkami i lukami:
    - Łączność
    - Inwentaryzacja sprzętu
    - Kontrola dostępu do sieci
    - Zdalna instalacja systemów operacyjnych
    - Zarządzaj lukami i poprawkami
    - Instalacja zdalna
    - Inwentaryzacja oprogramowania

Jeśli dla uprawnienia nie wybrano **Zezwól** ani **Odmów**, wówczas uprawnienie jest uznawane za *niezdefiniowane*: zostaje odrzucone, dopóki wyraźnie nie zostanie dozwolone lub odrzucone dla użytkownika.

Uprawnienia użytkownika są sumą:

- Własnych uprawnień użytkownika
- Uprawnień wszystkich ról przypisanych do tego użytkownika
- Uprawnień wszystkich grup bezpieczeństwa, do których należy użytkownik
- Uprawnień wszystkich ról przypisanych do grupy bezpieczeństwa, do których należy użytkownik

Jeśli przynajmniej jeden z tych zestawów uprawnień posiada opcję **Odmów** dla uprawnienia, wówczas dla użytkownika zostaje zabronione to uprawnienie nawet wtedy, gdy inne zestawy zezwalają na nie lub pozostawiają je niezdefiniowane.

Przydzielanie ról użytkownika do podrzędnych Serwerów administracyjnych

Domyślnie, listy ról użytkownika głównego i podrzędnego Serwera administracyjnego są niezależne. Możesz skonfigurować aplikację w taki sposób, aby automatycznie rozsyłała role użytkownika utworzone na głównym Serwerze administracyjnym do wszystkich podrzędnych Serwerów administracyjnych. Role użytkownika mogą także zostać rozesłane z podrzędnego Serwera administracyjnego na swoje własne podrzędne Serwery administracyjne.

W celu przesłania ról użytkownika z głównego Serwera administracyjnego na podrzędne Serwery administracyjne:

1. Otwórz okno główne aplikacji.
2. Wykonaj jedną z poniższych czynności:
   - W drzewie konsoli kliknij prawym klawiszem myszy nazwę Serwera administracyjnego i z otwartego menu kontekstowego wybierz **Właściwości**.
   - Jeśli posiadasz aktywny profil Serwera administracyjnego, w obszarze roboczym folderu **Profile** kliknij prawym klawiszem ten profil i z menu kontekstowego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego lub w oknie ustawień profilu, w panelu **Sekcje** wybierz **Role użytkownika**.

   Sekcja **Role użytkownika** jest dostępna, jeśli włączona jest opcja Wyświetl sekcje ustawień zabezpieczeń.
4. Włącz opcję **Przekaż listę ról do podrzędnych Serwerów administracyjnych**.
5. Kliknij **OK**.

Aplikacja kopiuje role użytkownika głównego Serwera administracyjnego na podrzędne Serwery administracyjne.

Jeśli opcja **Przekaż listę ról do podrzędnych Serwerów administracyjnych** jest włączona, a role użytkownika są przesyłane, nie mogą być edytowane ani usuwane na podrzędnych Serwerach administracyjnych. Jeśli tworzysz nową rolę lub edytujesz już tę istniejącą na głównym Serwerze administracyjnym, zmiany są automatycznie kopiowane do podrzędnych Serwerów administracyjnych. Jeśli usuwasz rolę użytkownika na głównym Serwerze administracyjnym, ta rola pozostanie na podrzędnych Serwerach administracyjnych, ale może być edytowana lub zostać usunięta.

Role, które zostają przesłane na podrzędny Serwer administracyjny z Serwera głównego, są wyświetlane z ikoną kłódki (🔒). Nie możesz edytować tych ról na podrzędnym Serwerze administracyjnym.

Jeśli tworzysz rolę na głównym Serwerze administracyjnym i istnieje rola z tą samą nazwą na swoim podrzędnym Serwerze administracyjnym, nowa rola zostaje skopiowana do podrzędnego Serwera administracyjnego z indeksem dodanym do jego nazwy, na przykład: ~~1, ~~2 (indeks może być losowy).

Jeśli wyłączysz opcję **Przekaż listę ról do podrzędnych Serwerów administracyjnych**, wszystkie role użytkownika pozostaną na podrzędnych Serwerach administracyjnych, ale staną się niezależne od tych na głównym Serwerze administracyjnym. Po tym, jak role użytkownika staną się niezależne, role użytkownika na podrzędnych Serwerach administracyjnych mogą być edytowane lub usuwane.

Wskazywanie użytkownika jako właściciela urządzenia

Możesz wskazać użytkownika jako właściciela urządzenia, aby przypisać urządzenie do tego użytkownika. Jeśli musisz wykonać jakiekolwiek działania na urządzeniu (na przykład zaktualizować oprogramowanie), administrator może poinformować właściciela urządzenia, aby autoryzował te działania.

W celu wskazania użytkownika jako właściciela urządzenia:

1. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.
2. W obszarze roboczym folderu, na zakładce **Urządzenia** wybierz urządzenie, dla którego chcesz wskazać właściciela.
3. Z otwartego menu kontekstowego urządzenia wybierz **Właściwości**.
4. W oknie właściwości urządzenia wybierz **Informacje o systemie** → **Sesje**.
5. Kliknij przycisk **Przypisz** znajdujący się obok pola **Właściciel urządzenia**.
6. W oknie **Wybór użytkownika** wybierz użytkownika, którego chcesz wskazać jako właściciela urządzenia, i kliknij **OK**.
7. Kliknij **OK**.

Właściciel urządzenia zostanie przypisany. Domyślnie pole **Właściciel urządzenia** jest uzupełnione wartością z Active Directory i jest aktualizowane podczas każdego przeszukiwania Active Directory. Listę właścicieli urządzeń możesz sprawdzić w **Raporcie dotyczącym właścicieli urządzeń**. Raport można utworzyć przy użyciu kreatora tworzenia nowego raportu.

Dostarczanie wiadomości użytkownikom

W celu wysyłania wiadomości do użytkownika za pośrednictwem poczty elektronicznej:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz użytkownika.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.
2. Z menu kontekstowego użytkownika wybierz **Powiadom przez e-mail**.
3. W oknie **Wysłanie wiadomości do użytkownika** uzupełnij odpowiednie pola, a następnie kliknij przycisk **OK**.

Wiadomość zostanie wysłana na adres e-mail określony we właściwościach użytkownika.

W celu wysyłania wiadomości SMS do użytkownika:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz użytkownika.
2. W menu kontekstowym użytkownika wybierz **Wyślij SMS**.
3. Uzupełnij odpowiednie pola w oknie **Treść SMS-a** i kliknij przycisk **OK**.

Wiadomość zostanie wysłana na urządzenie mobilne o numerze określonym we właściwościach użytkownika.

Przeglądanie listy urządzeń mobilnych użytkownika

W celu przejrzenia listy urządzeń mobilnych użytkownika:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz użytkownika.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Z menu kontekstowego konta użytkownika wybierz **Właściwości**.

3. W oknie właściwości konta użytkownika wybierz sekcję **Urządzenia mobilne**.

W sekcji **Urządzenia mobilne** możesz wyświetlić listę urządzeń mobilnych użytkownika oraz informacje o każdym z tych urządzeń. Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę urządzeń mobilnych do pliku.

Instalowanie certyfikatu dla użytkownika

Możesz zainstalować trzy certyfikaty dla użytkownika:

- Certyfikat współdzielony, który jest wymagany do identyfikacji urządzenia mobilnego użytkownika.
- Certyfikat poczty, który jest niezbędny do skonfigurowania poczty firmowej na urządzeniu mobilnym użytkownika.
- Certyfikat VPN, który jest niezbędny do skonfigurowania wirtualnej sieci prywatnej na urządzeniu mobilnym użytkownika.

W celu wydania certyfikatu dla użytkownika i jego zainstalowania:

1. W drzewie konsoli otwórz folder **Konta użytkowników** i wybierz konto użytkownika.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Z menu kontekstowego konta użytkownika wybierz **Zainstaluj certyfikat**.

   Zostanie uruchomiony kreator instalacji certyfikatu. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora instalacji certyfikatu, certyfikat zostanie utworzony i zainstalowany. Listę zainstalowanych certyfikatów użytkownika można przejrzeć oraz wyeksportować do pliku.

Wyświetlanie listy certyfikatów wydanych dla użytkownika

W celu wyświetlenia listy certyfikatów wydanych dla użytkownika:

1. Z drzewa konsoli, w folderze **Konta użytkowników** wybierz użytkownika.

   Domyślnie folder **Konta użytkowników** jest podfolderem folderu **Zaawansowane**.

2. Z menu kontekstowego konta użytkownika wybierz **Właściwości**.

3. W oknie właściwości konta użytkownika wybierz sekcję **Certyfikaty**.

W sekcji **Certyfikaty** możesz wyświetlić listę certyfikatów użytkownika oraz informacje o każdym z tych certyfikatów. Kliknij przycisk **Eksportuj do pliku**, aby zapisać listę certyfikatów do pliku.

Informacje o administratorze wirtualnego Serwera administracyjnego

Administrator sieci firmowej zarządzanej poprzez wirtualny Serwer administracyjny uruchamia Kaspersky Security Center Web Console z poziomu konta użytkownika określonego w tym oknie, aby wyświetlić szczegóły ochrony antywirusowej.

Jeśli jest to konieczne, na Serwerze wirtualnym można utworzyć kilka kont administratora.

Administrator wirtualnego Serwera Administracyjnego jest wewnętrznym użytkownikiem Kaspersky Security Center. Do systemu operacyjnego nie są przesyłane żadne dane dotyczące wewnętrznych użytkowników. Kaspersky Security Center autoryzuje wewnętrznych użytkowników.

Zdalna instalacja systemów operacyjnych i aplikacji

Kaspersky Security Center umożliwia tworzenie obrazów systemów operacyjnych i instalowanie ich na urządzeniach klienckich w sieci, a także wykonywanie zdalnej instalacji aplikacji firmy Kaspersky lub innych producentów.

Aby tworzyć obrazy systemów operacyjnych, musisz zainstalować Windows ADK i dodatek Windows PE dla Windows ADK na Serwerze administracyjnym. Zalecamy zainstalowanie najnowszych wersji zestawu Windows ADK i dodatku Windows PE dla zestawu Windows ADK. Możesz utworzyć obraz dowolnej wersji systemu operacyjnego Windows, która spełnia wymagania Kaspersky Security Center.

Przechwytywanie obrazów systemów operacyjnych

Kaspersky Security Center może przechwytywać obrazy systemów operacyjnych z urządzeń i przesyłać je do Serwera administracyjnego. Takie obrazy systemów operacyjnych są przechowywane na Serwerze administracyjnym w dedykowanym folderze. Obraz systemu operacyjnego odpowiedniego urządzenia może zostać przechwycony i utworzony przy użyciu zadania tworzenia pakietu instalacyjnego.

Funkcja przechwytywania obrazu systemu operacyjnego posiada następujące cechy:

- Obraz systemu operacyjnego nie może zostać przechwycony na urządzeniu z zainstalowanym Serwerem administracyjnym.
- Podczas przechwytywania obrazu systemu operacyjnego narzędzie sysprep.exe resetuje ustawienia odpowiedniego urządzenia. Jeśli chcesz przywrócić ustawienia urządzenia referencyjnego, zaznacz pole wyboru **Utwórz kopię zapasową stanu urządzenia** w kreatorze tworzenia zadania OS Imaging.
- Proces przechwytywania obrazu umożliwia ponowne uruchomienie odpowiedniego urządzenia.

Instalowanie obrazów systemów operacyjnych na nowych urządzeniach

Możesz użyć przechwyconych obrazów do zainstalowania ich na nowych urządzeniach w sieci, na których nie zainstalowano jeszcze systemu operacyjnego. W tym przypadku wykorzystywana jest technologia Preboot eXecution Environment (PXE). Wybierz w sieci urządzenie, które będzie używane jako serwer PXE. Urządzenie musi spełniać następujące wymagania:

- Na urządzeniu powinien zostać zainstalowany Agent sieciowy.
- Na urządzeniu nie może być aktywny żaden serwer DHCP, ponieważ serwer PXE używa tych samych portów co serwer DHCP.
- Segment sieci, który zawiera urządzenie, nie powinien zawierać innych serwerów PXE.

W celu zainstalowania systemu operacyjnego należy spełnić następujące warunki:

- W urządzeniu powinna znajdować się karta sieciowa.
- Urządzenie musi być połączone z siecią.
- Podczas uruchamiania urządzenia, w BIOS-ie należy wybrać opcję Network boot.

Zdalna instalacja systemów operacyjnych odbywa się w następujący sposób:

1. Podczas uruchamiania serwer PXE nawiązuje połączenie z nowym urządzeniem klienckim.
2. Urządzenie klienckie zostaje włączone do środowiska Windows Preinstallation Environment (WinPE).

   Włączenie urządzenia do środowiska WinPE może wymagać konfiguracji zestawu sterowników dla WinPE.

3. Urządzenie klienckie jest rejestrowane na Serwerze administracyjnym.
4. Administrator przypisuje do urządzenia klienckiego pakiet instalacyjny z obrazem systemu operacyjnego.

   Administrator może dodać żądane sterowniki do pakietu instalacyjnego z obrazem systemu operacyjnego. Administrator może także określić plik konfiguracji z ustawieniami systemu operacyjnego (plik odpowiedzi), który będzie stosowany podczas instalacji.

5. System operacyjny zostanie zainstalowany na urządzeniu klienckim.

Administrator może ręcznie określić adresy MAC urządzeń klienckich, które nie zostały jeszcze połączone, i przypisać do nich pakiet instalacyjny z obrazem systemu operacyjnego. Po połączeniu wybranych urządzeń klienckich z serwerem PXE, system operacyjny jest automatycznie instalowany na tych urządzeniach.

Instalowanie obrazów systemów operacyjnych na urządzeniach, na których zainstalowany jest już inny system operacyjny

Zdalna instalacja obrazów systemów operacyjnych na urządzeniach klienckich, na których zainstalowany jest już inny system operacyjny, odbywa się poprzez zadanie zdalnej instalacji dla określonych urządzeń.

Instalowanie aplikacji firmy Kaspersky i innych producentów

Administrator może utworzyć pakiety instalacyjne dowolnych aplikacji, łącznie z tymi określonymi przez użytkownika, oraz zainstalować aplikacje na urządzeniach klienckich przy użyciu zadania zdalnej instalacji.

Tworzenie obrazów systemów operacyjnych

Obrazy systemów operacyjnych są tworzone przy użyciu zadania usuwania obrazu systemu operacyjnego odpowiedniego urządzenia.

W celu utworzenia zadania tworzenia obrazu systemu operacyjnego:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Kliknij przycisk **Utwórz pakiet instalacyjny**, aby uruchomić Kreator tworzenia nowego pakietu.
3. W oknie **Wybierz typ pakietu instalacyjnego** kliknij przycisk **Utwórz pakiet instalacyjny zawierający obraz systemu operacyjnego**.
4. Postępuj zgodnie z instrukcjami kreatora.

   Po zakończeniu pracy kreatora, zostaje utworzone zadanie Serwera administracyjnego o nazwie **Tworzenie pakietu instalacyjnego bazującego na obrazie systemu operacyjnego zainstalowanego na urządzeniu**. Zadanie można zobaczyć w folderze **Zadania**.

Po zakończeniu wykonywania zadania **Tworzenie pakietu instalacyjnego bazującego na obrazie systemu operacyjnego zainstalowanego na urządzeniu** tworzony jest pakiet instalacyjny, który może zostać użyty do zainstalowania systemu operacyjnego na urządzeniach klienckich poprzez serwer PXE lub zadanie zdalnej instalacji. Pakiet instalacyjny można zobaczyć w folderze **Pakiety instalacyjne**.

Instalowanie obrazów systemów operacyjnych

Kaspersky Security Center umożliwia instalację obrazów WIM pulpitu i serwerowych systemów operacyjnych Windows® na urządzeniach w sieci organizacji.

W celu uzyskania obrazu systemu operacyjnego, który będzie mógł zostać zainstalowany przy użyciu narzędzi Kaspersky Security Center:

- Zaimportuj obraz z pliku install.wim znajdującego się w pakiecie dystrybucyjnym systemu Windows
- Przechwyć obraz z urządzenia odniesienia

Dla instalacji obrazów systemu operacyjnego są obsługiwane dwa scenariusze:

- Zdalna instalacja na "czystym" urządzeniu, na którym nie ma zainstalowanego systemu operacyjnego
- Zdalna instalacja na urządzeniu działającym pod kontrolą systemu Windows

Serwer administracyjny zawiera obraz środowiska preinstalacyjnego systemu Windows (Windows PE), który jest zawsze używany do przechwytywania obrazów systemu operacyjnego oraz do ich instalowania. Wszystkie sterowniki niezbędne do właściwego funkcjonowania wszystkich urządzeń docelowych muszą zostać dodane do obrazu WinPE. Zazwyczaj też należy dodać sterowniki mikroukładu, aby interfejs sieci Ethernet działał poprawnie.

W celu zaimplementowania scenariuszy przechwytywania i instalacji obrazu muszą być spełnione następujące warunki:

- Na Serwerze administracyjnym musi być zainstalowany Zestaw zautomatyzowanej instalacji systemu Windows (Windows WAIK) w wersji 2.0 (lub nowszej) bądź Zestaw do oceny i wdrażania systemu Windows (Windows WADK). Jeśli scenariusz przewiduje instalowanie i przechwytywanie obrazów na systemie Windows XP, należy zainstalować Windows WAIK.

- W sieci, w której znajduje się urządzenie docelowe, musi być dostępny serwer DHCP.

- Folder współdzielony Serwera administracyjnego musi zostać otwarty do odczytu w sieci, w której znajduje się urządzenie docelowe. Jeśli folder współdzielony znajduje się na Serwerze administracyjnym, wymagany jest dostęp dla konta KlPxeUser (to konto jest tworzone automatycznie podczas działania instalatora Serwera administracyjnego). Jeśli folder współdzielony znajduje się poza Serwerem administracyjnym, uprawnienie dostępu musi zostać nadane każdemu.

Podczas wybierania instalowanego obrazu systemu operacyjnego administrator musi wyraźnie określić architekturę procesora urządzenia docelowego: x86 lub x86-64.

Konfigurowanie adresu serwera proxy KSN

Domyślnie, nazwa domeny Serwera administracyjnego pokrywa się z adresem serwera proxy KSN. Jeśli zmienisz nazwę domeny dla Serwera administracyjnego, musisz określić poprawny adres serwera proxy KSN, aby zapobiec utracie połączenia między hostem a KSN.

W celu skonfigurowania adresu serwera proxy KSN:

1. W drzewie konsoli przejdź do **Zaawansowane** → **Zdalna instalacja** → **Pakiety instalacyjne**.
2. Z menu kontekstowego **Pakiety instalacyjne** wybierz **Właściwości**.
3. W otwartym oknie, na zakładce **Ogólny** określ nowy adres serwera proxy KSN.
4. Kliknij przycisk **Zastosuj**.

Od teraz określany adres jest używany jako adres serwera proxy KSN.

Dodawanie sterowników dla Windows Preinstallation Environment (WinPE)

W celu dodania sterowników dla Windows Preinstallation Environment (WinPE):

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Wdrażanie obrazów urządzenia**.
2. W obszarze roboczym folderu **Wdrażanie obrazów urządzenia** kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Konfiguruj zestaw sterowników Środowiska preinstalacji systemu Windows (WinPE)**.

   Zostanie otwarte okno **Sterowniki środowiska preinstalacji systemu Windows**.
3. W oknie **Sterowniki środowiska preinstalacji systemu Windows** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Wybierz sterownik**.
4. W oknie **Wybierz sterownik** wybierz sterownik z listy.

Jeśli na liście nie ma żądanego sterownika, kliknij przycisk **Dodaj** i określ nazwę sterownika oraz folder pakietu dystrybucyjnego sterownika w oknie **Dodaj sterownik**, które zostanie otwarte.

Możesz wybrać folder, klikając przycisk **Przeglądaj**.

W oknie **Dodaj sterownik** kliknij **OK**.

5. W oknie **Wybierz sterownik** kliknij **OK**.

   Sterownik zostanie dodany do repozytorium Serwera administracyjnego. Po dodaniu do repozytorium, sterownik jest wyświetlany w oknie **Wybierz sterownik**.

6. W oknie **Sterowniki środowiska preinstalacji systemu Windows** kliknij **OK**.

Sterownik zostanie dodany do Windows Preinstallation Environment (WinPE).

Dodawanie sterowników do pakietu instalacyjnego z obrazem systemu operacyjnego

W celu dodania sterowników do pakietu instalacyjnego z obrazem systemu operacyjnego:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Z menu kontekstowego pakietu instalacyjnego z obrazem systemu operacyjnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości pakietu instalacyjnego.

3. W oknie właściwości pakietu instalacyjnego wybierz sekcję **Dodatkowe sterowniki**.
4. Kliknij przycisk **Dodaj** w sekcji **Dodatkowe sterowniki**.

   Zostanie otwarte okno **Wybierz sterownik**.

5. W oknie **Wybierz sterownik** wybierz sterowniki, które chcesz dodać do pakietu instalacyjnego z obrazem systemu operacyjnego.

   Nowe sterowniki można dodać do repozytorium Serwera administracyjnego, klikając przycisk **Dodaj** dostępny w oknie **Wybierz sterownik**.

6. Kliknij **OK**.

Dodane sterowniki są wyświetlane w sekcji **Dodatkowe sterowniki** okna właściwości pakietu instalacyjnego z obrazem systemu operacyjnego.

Konfigurowanie narzędzia sysprep.exe

Narzędzie sysrep.exe jest przeznaczone do przygotowania urządzenia do utworzenia obrazu systemu operacyjnego.

W celu skonfigurowania narzędzia sysprep.exe:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Z menu kontekstowego pakietu instalacyjnego z obrazem systemu operacyjnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości pakietu instalacyjnego.

3. W oknie właściwości pakietu instalacyjnego wybierz sekcję **Ustawienia sysprep.exe**.

4. W sekcji **Ustawienia sysprep.exe** określ plik konfiguracyjny, który zostanie użyty podczas instalacji systemu operacyjnego na urządzeniu klienckim:

   - **Użyj domyślnego pliku konfiguracyjnego**. Wybierz tę opcję, aby użyć pliku odpowiedzi, domyślnie wygenerowanego podczas przechwytywania obrazu systemu operacyjnego.
   - **Określ niestandardowe wartości głównych ustawień**. Wybierz tę opcję, aby określić wartości dla ustawień poprzez interfejs.
   - **Określ plik konfiguracyjny**. Wybierz tę opcję, aby użyć niestandardowego pliku odpowiedzi.

5. W celu zastosowania wprowadzonych zmian należy kliknąć przycisk **Zastosuj**.

Instalowanie systemów operacyjnych na urządzeniach w sieci

W celu zainstalowania systemu operacyjnego na nowych urządzeniach, na których jeszcze nie zainstalowano żadnego systemu operacyjnego:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Wdrażanie obrazów urządzenia**.
2. Kliknij przycisk **Akcje dodatkowe** i z listwy rozwijalnej wybierz **Zarządzaj listą serwerów PXE znajdujących się w sieci**.

   Zostanie otwarte okno **Właściwości: Rozsyłanie obrazów urządzenia** na sekcji **Serwery PXE**.
3. W sekcji **Serwery PXE** kliknij przycisk **Dodaj** i w oknie **Serwery PXE**, które zostanie otwarte, wybierz urządzenie, które będzie używane jako serwer PXE.

   Urządzenie, które dodałeś, jest wyświetlone w sekcji Serwery PXE.
4. W sekcji **Serwery PXE** wybierz serwer PXE i kliknij przycisk **Właściwości**.
5. W oknie właściwości wybranego serwera PXE, na zakładce **Ustawienia połączenia z serwerem PXE** skonfiguruj połączenie między Serwerem administracyjnym a serwerem PXE.
6. Uruchom urządzenie klienckie, na którym chcesz zainstalować system operacyjny.
7. W BIOS-ie urządzenia klienckiego wybierz opcję Network boot.

   Urządzenie klienckie nawiąże połączenie z serwerem PXE, a następnie jest wyświetlane w obszarze roboczym folderu **Wdrażanie obrazów urządzenia**.
8. W sekcji **Akcje** kliknij odnośnik **Przypisz pakiet instalacyjny**, aby wybrać pakiet instalacyjny, który zostanie użyty do zainstalowania systemu operacyjnego na wybranym urządzeniu.

   Po dodaniu urządzenia i przypisaniu do niego pakietu instalacyjnego, zdalna instalacja systemu operacyjnego zostanie automatycznie uruchomiona na tym urządzeniu.
9. Aby anulować zdalną instalację systemu operacyjnego na urządzeniu klienckim, w sekcji **Akcje** kliknij odnośnik **Anuluj instalację obrazu systemu operacyjnego**.

W celu dodania urządzeń według adresu MAC:

- W folderze **Wdrażanie obrazów urządzenia** kliknij **Dodaj adres MAC urządzenia**, aby otworzyć okno **Nowe urządzenie**, w którym określ adres MAC urządzenia, które chcesz dodać.

- W folderze **Wdrażanie obrazów urządzenia** kliknij **Importuj adresy MAC urządzeń z pliku**, aby wybrać plik zawierający listę adresów MAC wszystkich urządzeń, na których chcesz zainstalować system operacyjny.

Instalowanie systemów operacyjnych na urządzeniach klienckich

W celu zainstalowania systemu operacyjnego na urządzeniach klienckich, na których jest już zainstalowany inny system operacyjny:

1. W drzewie konsoli otwórz folder **Zdalna instalacja** i kliknij odnośnik **Roześlij pakiet instalacyjny na zarządzane urządzenia (stacje robocze)**, aby uruchomić Kreator wdrażania ochrony.
2. W oknie **Wybierz pakiet instalacyjny** wskaż pakiet instalacyjny z obrazem systemu operacyjnego.
3. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora, zostanie utworzone zadanie zdalnej instalacji dla instalacji systemu operacyjnego na urządzeniach klienckich. Zadanie może zostać uruchomione lub zatrzymane w folderze **Zadania**.

Tworzenie pakietów instalacyjnych aplikacji

W celu utworzenia pakietu instalacyjnego aplikacji:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.
2. Kliknij przycisk **Utwórz pakiet instalacyjny**, aby uruchomić Kreator tworzenia nowego pakietu.
3. W oknie **Wybierz typ pakietu instalacyjnego** kliknij jeden z następujących przycisków:
   - **Utwórz pakiet instalacyjny dla aplikacji Kaspersky**. Wybierz tę opcję, jeśli chcesz utworzyć pakiet instalacyjny dla aplikacji Kaspersky.
   - **Utwórz pakiet instalacyjny dla określonego pliku wykonywalnego**. Wybierz tę opcję, jeśli chcesz utworzyć pakiet instalacyjny dla aplikacji innej firmy przy użyciu pliku wykonywalnego. Zazwyczaj plik wykonywalny to plik instalacyjny aplikacji.
     - Kopiuj całą zawartość folderu do pakietu instalacyjnego

       Wybierz tę opcję, jeśli plikowi wykonywalnemu towarzyszą dodatkowe pliki wymagane do zainstalowania aplikacji. Przed włączeniem tej opcji upewnij się, że wszystkie wymagane pliki są przechowywane w tym samym folderze. Jeśli ta opcja jest włączona, aplikacja doda całą zawartość folderu, w tym określony plik wykonywalny, do pakietu instalacyjnego.

     - Określ parametry instalacji

Aby zdalna instalacja zakończyła się pomyślnie, dla większości aplikacji wymagane jest wykonanie instalacji w trybie cichym. W takim przypadku należy określić parametr dla cichej instalacji.

Skonfiguruj ustawienia instalacji:

- **Wiersz polecenia pliku wykonywalnego**

  Jeśli dla cichej instalacji aplikacja wymaga dodatkowych parametrów, określ je w tym polu. Więcej informacji można znaleźć w dokumentacji producenta.

  Możesz też wprowadzić inne parametry.

- **Konwertuj ustawienia na zalecane wartości dla aplikacji rozpoznawanych przez Kaspersky Security Center**

  Aplikacja zostanie zainstalowana z zalecanymi ustawieniami, jeśli informacje o określonej aplikacji znajdują się w bazie danych Kaspersky.

  Jeśli wprowadziłeś parametry w polu **Wiersz polecenia pliku wykonywalnego**, zostaną zapisane z zalecanymi ustawieniami.

  Domyślnie opcja ta jest włączona.

  Baza danych Kaspersky jest tworzona i zarządzana przez analityków z Kaspersky. Dla każdej aplikacji dodanej do bazy danych analitycy z Kaspersky definiują optymalne ustawienia instalacji. Ustawienia są definiowane, aby zapewnić pomyślną zdalną instalację aplikacji na urządzeniu klienckim. Baza danych jest automatycznie aktualizowana na Serwerze administracyjnym, gdy uruchamiasz zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego.

- **Wybierz aplikację z bazy danych Kaspersky do utworzenia pakietu instalacyjnego**. Wybierz tę opcję, jeśli chcesz wybrać wymaganą aplikację innej firmy z bazy danych Kaspersky do utworzenia pakietu instalacyjnego. Baza danych jest tworzona automatycznie, gdy uruchamiasz zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego; aplikacje są wyświetlane na liście.

- **Utwórz pakiet instalacyjny zawierający obraz systemu operacyjnego**. Wybierz tę opcję, jeśli chcesz utworzyć pakiet instalacyjny z obrazem systemu operacyjnego odpowiedniego urządzenia.

  Po zakończeniu pracy kreatora, zostaje utworzone zadanie Serwera administracyjnego o nazwie **Utwórz pakiet instalacyjny na podstawie obrazu referencyjnego systemu operacyjnego urządzenia**. Po zakończeniu wykonywania zadania tworzony jest pakiet instalacyjny, który może zostać użyty do zainstalowania obrazu systemu operacyjnego poprzez serwer PXE lub zadanie zdalnej instalacji.

4. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora, zostanie utworzony pakiet instalacyjny, który może zostać użyty do zainstalowania aplikacji na urządzeniach klienckich. Możesz przejrzeć pakiet instalacyjny, wybierając **Pakiety instalacyjne** w drzewie konsoli.

Tworzenie certyfikatu dla pakietów instalacyjnych aplikacji

W celu utworzenia certyfikatu dla pakietu instalacyjnego aplikacji:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.

   Domyślnie folder **Zdalna instalacja** to podfolder folderu **Zaawansowane**.

2. Z menu kontekstowego folderu **Pakiety instalacyjne** wybierz **Zaawansowane**.

To spowoduje otwarcie okna właściwości folderu **Pakiety instalacyjne**.

3. W oknie właściwości folderu **Pakiety instalacyjne** wybierz sekcję **Podpisz pakiety autonomiczne**.
4. W sekcji **Podpisz pakiety autonomiczne** kliknij przycisk **Określ**.
   Okno **Certyfikat**.
5. W polu **Typ certyfikatu** określ typ certyfikatu - publiczny lub prywatny:
   - Jeśli wybrana jest wartość **Kontener PKCS #12**, określ plik certyfikatu i hasło.
   - Jeśli wybrana jest wartość **Certyfikat X.509**:
     a. Określ plik klucza prywatnego (z rozszerzeniem *.prk lub *.pem).
     b. Określ hasło dla klucza prywatnego.
     c. Określ plik klucza publicznego (z rozszerzeniem *.cer).
6. Kliknij **OK**.

Zostanie utworzony certyfikat dla pakietu instalacyjnego aplikacji.

Instalowanie aplikacji na urządzeniach klienckich

W celu zainstalowania aplikacji na urządzeniach klienckich:

1. W drzewie konsoli otwórz folder **Zdalna instalacja** i kliknij **Roześlij pakiet instalacyjny na zarządzane urządzenia (stacje robocze)**, aby uruchomić Kreator wdrażania ochrony.
2. W oknie **Wybierz pakiet instalacyjny** wskaż pakiet instalacyjny aplikacji, którą chcesz zainstalować.
3. Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora, zostanie utworzone zadanie zdalnej instalacji dla instalacji aplikacji na urządzeniach klienckich. Zadanie może zostać uruchomione lub zatrzymane w folderze **Zadania**.

Użyj kreatora wdrażania ochrony, aby zainstalować Agenta sieciowego na urządzeniach klienckich działających pod kontrolą systemów Windows, Linux i macOS.

Aby zarządzać 64-bitowymi aplikacjami zabezpieczającymi przy użyciu Kaspersky Security Center na urządzeniach działających pod kontrolą systemu operacyjnego Linux, należy użyć 64-bitowej wersji Agenta sieciowego dla systemu Linux. Żądaną wersję Agenta sieciowego można pobrać ze strony internetowej pomocy technicznej.

Przed zdalną instalacją Agenta sieciowego na urządzeniu z systemem Linux należy przygotować urządzenie.

Zarządzanie rewizjami obiektów

Ta sekcja zawiera informacje dotyczące zarządzania rewizjami obiektów. Kaspersky Security Center umożliwia śledzenie modyfikacji obiektów. Za każdym razem, gdy zapisujesz zmiany wprowadzone w obiekcie, tworzona jest *rewizja*. Każda rewizja posiada numer.

Obiekty aplikacji, które obsługują zarządzanie rewizjami, obejmują:

- Serwery administracyjne
- Zasady
- Zadania
- Grupy administracyjne
- Konta użytkowników
- Pakiety instalacyjne

Na rewizjach obiektów możesz wykonać następujące działania:

- Porównać wybraną rewizję z bieżącą rewizją
- Porównać wybrane rewizje
- Porównać obiekt wybranej rewizji z innym obiektem tego samego typu
- Przejrzeć wybraną rewizję
- Wycofać zmiany wprowadzone w obiekcie do wybranej rewizji
- Zapisać rewizje jako plik .txt

W oknie właściwości dowolnego obiektu obsługującego zarządzanie rewizjami sekcja **Historia rewizji** wyświetla listę rewizji obiektów z następującymi szczegółami:

- Liczbę rewizji obiektu
- Datę i godzinę modyfikacji obiektu
- Nazwę użytkownika, który zmodyfikował obiekt
- Działanie wykonane na obiekcie
- Opis rewizji związanej ze zmianą wprowadzoną w ustawieniach obiektu

  Domyślnie, pole opisu rewizji obiektu jest puste. Aby dodać opis do rewizji, wybierz żądaną rewizję i kliknij przycisk **Opis**. W oknie **Opis rewizji obiektu** wprowadź opis rewizji.

Informacje o rewizjach obiektów

Na rewizjach obiektów możesz wykonać następujące działania:

- Porównać wybraną rewizję z bieżącą rewizją
- Porównać wybrane rewizje
- Porównać obiekt wybranej rewizji z innym obiektem tego samego typu
- Przejrzeć wybraną rewizję
- Wycofać zmiany wprowadzone w obiekcie do wybranej rewizji
- Zapisać rewizje jako plik .txt

W oknie właściwości dowolnego obiektu obsługującego zarządzanie rewizjami sekcja **Historia rewizji** wyświetla listę rewizji obiektów z następującymi szczegółami:

- Liczbę rewizji obiektu
- Datę i godzinę modyfikacji obiektu
- Nazwę użytkownika, który zmodyfikował obiekt
- Działanie wykonane na obiekcie
- Opis rewizji związanej ze zmianą wprowadzoną w ustawieniach obiektu

Przeglądanie sekcji Historia rewizji

Możesz porównać rewizje obiektu z bieżącą rewizją, porównać różne rewizje wybrane na liście lub porównać rewizję obiektu z rewizją innego obiektu tego samego typu.

*W celu przejrzenia sekcji **Historia rewizji** obiektu:*

1. W drzewie konsoli wybierz jeden z następujących obiektów:
   - Węzeł **Serwer administracyjny**
   - Folder **Zasady**
   - Folder **Zadania**
   - Folder grupy administracyjnej
   - Folder **Konta użytkowników**
   - Folder **Usunięte obiekty**
   - Podfolder **Pakiety instalacyjne**, który jest zagnieżdżony w folderze **Zdalna instalacja**
2. W zależności od lokalizacji żądanego obiektu, wykonaj jedną z następujących czynności:

- Jeśli obiekt znajduje się w węźle **Serwera administracyjnego** lub w węźle grupy administracyjnej, kliknij węzeł prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.
- Jeśli obiekt znajduje się w folderze **Zasady**, **Zadania**, **Konta użytkowników**, **Usunięte obiekty**, lub **Pakiety instalacyjne**, wybierz folder, a w odpowiednim obszarze roboczym wybierz obiekt.

Zostanie otwarte okno właściwości obiektu.

3. W lewym panelu **Sekcje** wybierz **Historia rewizji**.

Historia rewizji jest wyświetlana w obszarze roboczym.

Porównywanie rewizji obiektu

Możesz porównać poprzednie rewizje obiektu z bieżącą rewizją, porównać różne rewizje wybrane na liście lub porównać rewizję obiektu z rewizją innego obiektu tego samego typu.

W celu porównania rewizji obiektu:

1. Wybierz obiekt i przejdź do okna właściwości obiektu.
2. W oknie właściwości przejdź do sekcji **Historia rewizji**.
3. W obszarze roboczym, na liście rewizji obiektu wybierz rewizję do porównania.

   Aby wybrać więcej niż jedną rewizję obiektu, użyj klawiszy **`Shift`** i **`Ctrl`**.
4. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk podziału **Porównaj** i z listy rozwijalnej wybierz jedną z wartości:
     - **Porównaj z bieżącą rewizją**

       Wybierz tę opcję, aby porównać wybraną rewizję z bieżącą rewizją.
     - **Porównaj wybrane rewizje**

       Wybierz tę opcję, aby porównać dwie wybrane rewizje.
     - **Porównaj z innym zadaniem**

       Jeśli pracujesz z rewizjami zadania, wybierz **Porównaj z innym zadaniem**, aby porównać wybraną rewizję z rewizją innego zadania.

       Jeśli pracujesz z rewizjami profilu, wybierz **Porównaj z inną zasadą**, aby porównać wybraną rewizję z rewizją innego profilu.
   - Kliknij dwukrotnie nazwę rewizji i w otwartym oknie właściwości rewizji kliknij jeden z następujących przycisków:
     - **Porównaj z bieżącą**

Kliknij ten przycisk, aby porównać wybraną rewizję z bieżącą rewizją.

- **Porównaj z poprzednią**

  Kliknij ten przycisk, aby porównać wybraną rewizję z poprzednią rewizją.

W domyślnej przeglądarce zostanie wyświetlony raport w formacie HTML z porównaniem rewizji.

W tym raporcie możesz zminimalizować niektóre sekcje zawierające ustawienia rewizji. Aby zminimalizować sekcję z ustawieniami rewizji obiektu, kliknij ikonę strzałki (▲) obok nazwy sekcji.

Rewizje Serwera administracyjnego zawierają wszystkie szczegóły dotyczące wprowadzonych zmian, za wyjątkiem szczegółów z następujących obszarów:

- Sekcja **Ruch sieciowy**
- Sekcja **Reguły znakowania**
- Sekcja **Powiadamianie**
- Sekcja **Punkty dystrybucji**
- Sekcja **Epidemia wirusa**

  Z sekcji **Epidemia wirusa** nie są zapisywane żadne informacje o konfiguracji aktywacji profilu, która nastąpiła, gdy zdarzenie Epidemia wirusa zostało wyzwolone.

Możesz porównać rewizje usuniętego obiektu z rewizją istniejącego obiektu, ale nie odwrotnie: nie możesz porównać rewizji istniejącego obiektu z rewizją usuniętego obiektu.

Określanie czasu przechowywania rewizji obiektu oraz informacji o usuniętym obiekcie

Okres przechowywania rewizji obiektu i informacji o usuniętych obiektach jest taki sam. Domyślnie okres przechowywania wynosi 90 dni. Jest to wystarczający czas na przeprowadzenie regularnego audytu programu.

Tylko użytkownicy z uprawnieniem **Modyfikacja** w obszarze uprawnień **Usunięte obiekty** mogą zmienić okres przechowywania.

W celu zmiany okresu przechowywania rewizji obiektu i informacji o usuniętych obiektach:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz zmienić okres przechowywania.
2. W menu kontekstowym kliknij prawym klawiszem myszy i wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, które zostanie otwarte, w sekcji **Repozytorium historii rewizji** wprowadź żądany okres przechowywania (liczba dni).
4. Kliknij **OK**.

Rewizje obiektu i informacje o usuniętych obiektach będą przechowywane przez liczbę dni, którą wprowadziłeś.

Przeglądanie rewizji obiektu

Jeśli chcesz wiedzieć, jakie modyfikacje zostały wprowadzone w obiekcie w określonym przedziale czasu, możesz przejrzeć rewizje tego obiektu.

W celu przejrzenia rewizji obiektu:

1. Przejdź do sekcji **Historia rewizji** obiektu.
2. Na liście rewizji obiektu wybierz rewizję, której ustawienia chcesz przejrzeć.
3. Wykonaj jedną z poniższych czynności:
   - Kliknij przycisk **Wyświetl rewizję**.
   - Otwórz okno właściwości rewizji, klikając dwukrotnie nazwę rewizji, a następnie klikając przycisk **Wyświetl rewizję**.

Zostanie wyświetlony raport w formacie HTML zawierający ustawienia wybranej rewizji obiektu. W tym raporcie możesz zminimalizować niektóre sekcje z ustawieniami rewizji obiektu. Aby zminimalizować sekcję z ustawieniami rewizji obiektu, kliknij ikonę strzałki ( ) obok nazwy sekcji.

Zapisywanie rewizji obiektu do pliku

Rewizję obiektu możesz zapisać jako plik tekstowy, na przykład, aby wysłać go za pośrednictwem poczty elektronicznej.

W celu zapisania rewizji obiektu do pliku:

1. Przejdź do sekcji **Historia rewizji** obiektu.
2. Na liście rewizji obiektu wybierz tę, której ustawienia chcesz zapisać.
3. Kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz wartość **Zapisz do pliku**.

Rewizja zostanie zapisana do pliku .txt.

Wycofywanie zmian

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w obiekcie. Na przykład, konieczne może być przywrócenie ustawień profilu z określonego dnia.

W celu wycofania zmian wprowadzonych w obiekcie:

1. Przejdź do sekcji **Historia rewizji** obiektu.
2. Na liście rewizji obiektu wybierz numer rewizji, do której chcesz wycofać zmiany.
3. Kliknij przycisk **Zaawansowane** i z listy rozwijalnej wybierz wartość **Wycofaj**.

Obiekt zostanie wycofany do wybranej rewizji. Lista rewizji obiektu wyświetla wpis dotyczący podjętego działania. Opis rewizji wyświetla informacje o numerze rewizji, do której wycofałeś obiekt.

Dodawanie opisu rewizji

Możesz dodać opis dla rewizji, aby uprościć wyszukiwanie rewizji na liście.

W celu dodania opisu rewizji:

1. Przejdź do sekcji **Historia rewizji** obiektu.
2. Na liście rewizji obiektu wybierz rewizję, dla której chcesz dodać opis.
3. Kliknij przycisk **Opis**.
4. W oknie **Opis rewizji obiektu** wprowadź opis rewizji.
   Domyślnie, pole opisu rewizji obiektu jest puste.
5. Kliknij **OK**.

Usuwanie obiektów

Ta sekcja zawiera informacje dotyczące usuwania obiektów i przeglądania informacji o obiektach po ich usunięciu.

Możesz usuwać obiekty, w tym:

- Zasady
- Zadania
- Pakiety instalacyjne
- Wirtualne Serwery administracyjne
- Użytkownicy
- Grupy bezpieczeństwa
- Grupy administracyjne

Jeśli usuniesz obiekt, informacje o nim pozostaną w bazie danych. Okres przechowywania informacji o usuniętych obiektach jest taki sam, jak okres przechowywania rewizji obiektu (zalecany okres wynosi 90 dni). Możesz zmienić okres przechowywania tylko wtedy, gdy posiadasz uprawnienie **Modyfikacja** w obszarze uprawnień **Usunięte obiekty**.

Usuwanie obiektu

Możesz usuwać obiekty, takie jak profile, zadania, pakiety instalacyjne, użytkownicy wewnętrzni i grupy użytkowników wewnętrznych, jeśli masz uprawnienie Modyfikacja, które jest w kategorii Podstawowe funkcje uprawnień (więcej informacji znajdziesz w sekcji Przydzielanie uprawnień użytkownikom i grupom).

W celu usunięcia obiektu:

1. W drzewie konsoli, w obszarze roboczym żądanego folderu wybierz obiekt.
2. Wykonaj jedną z poniższych czynności:
   - Kliknij obiekt prawym klawiszem myszy i wybierz **Usuń**.
   - Wciśnij klawisz **DELETE**.

   Obiekt zostanie usunięty, a informacje o nim będą przechowywane w bazie danych.

Przeglądanie informacji o usuniętych obiektach

Informacje o usuniętych obiektach są przechowywane w folderze Usunięte obiekty przez ten sam czas, co rewizje obiektu (zalecany okres to 90 dni).

Tylko użytkownicy z uprawnieniem **Odczyt** w obszarze uprawnień **Usunięte obiekty** mogą przeglądać listę usuniętych obiektów (więcej informacji znajdziesz w sekcji Przydzielanie uprawnień użytkownikom i grupom).

W celu wyświetlenia listy usuniętych obiektów:

W drzewie konsoli wybierz **Usunięte obiekty** (domyślnie **Usunięte obiekty** to podfolder folderu **Zaawansowane**).

Jeśli nie masz uprawnienia Odczyt w obszarze uprawnień **Usunięte obiekty**, pusta lista jest wyświetlana w folderze **Usunięte obiekty**.

Obszar roboczy folderu **Usunięte obiekty** zawiera następujące informacje o usuniętych obiektach:

- **Nazwa**. Nazwa obiektu.
- **Typ**. Typ obiektu, taki jak profil, zadanie lub pakiet instalacyjny.
- **Czas**. Godzina usunięcia obiektu.
- **Użytkownik**. Nazwa konta użytkownika, który usunął obiekt.

W celu wyświetlenia więcej informacji o obiekcie:

1. W drzewie konsoli wybierz **Usunięte obiekty** (domyślnie **Usunięte obiekty** to podfolder folderu **Zaawansowane**).
2. W obszarze roboczym **Usunięte obiekty** wybierz obiekt, którego potrzebujesz.

   W prawej części obszaru roboczego pojawi się okno do pracy z wybranym obiektem.
3. Wykonaj jedną z poniższych czynności:
   - Kliknij odnośnik **Właściwości**, dostępny w oknie.

- Kliknij prawym klawiszem myszy obiekt, który wybrałeś w obszarze roboczym, a w menu kontekstowym wybierz **Właściwości**.

Zostanie otwarte okno właściwości obiektu, wyświetlające następujące zakładki:

- **Ogólny**
- **Historia rewizji**

Trwałe usuwanie obiektów z listy usuniętych obiektów

Tylko użytkownicy z uprawnieniem **Modyfikacja** w obszarze uprawnień **Usunięte obiekty** mogą trwale usuwać obiekty z listy usuniętych obiektów (więcej informacji znajdziesz w sekcji Przydzielanie uprawnień użytkownikom i grupom).

W celu usunięcia obiektu z listy usuniętych obiektów:

1. W drzewie konsoli wybierz węzeł żądanego Serwera administracyjnego, a następnie wybierz folder **Usunięte obiekty**.
2. W obszarze roboczym wybierz obiekt(y), który chcesz usunąć.
3. Wykonaj jedną z poniższych czynności:
   - Wciśnij klawisz **DELETE**.
   - W menu kontekstowym wybranego obiektu(ów) wybierz **Usuń**.
4. W oknie potwierdzenia kliknij **Tak**.

Obiekt zostaje trwale usunięty z listy usuniętych obiektów. Wszystkie informacje o tym obiekcie (w tym wszystkich jego rewizjach) zostają trwale usunięte z bazy danych. Nie możesz odzyskać tych informacji.

Zarządzanie urządzeniami mobilnymi

Zarządzanie ochroną urządzeń mobilnych poprzez Kaspersky Security Center jest realizowane przy użyciu funkcji Zarządzanie urządzeniami mobilnymi, która wymaga dedykowanej licencji. Jeśli zamierzasz zarządzać urządzeniami mobilnymi należącymi do pracowników Twojej organizacji, musisz włączyć Zarządzanie urządzeniami mobilnymi.

Ta sekcja zawiera instrukcja włączania, konfigurowania i wyłączania Zarządzania urządzeniami mobilnymi. W tej sekcji można znaleźć także opis sposobu zarządzania urządzeniami mobilnymi podłączonymi do Serwera administracyjnego.

Więcej informacji o Kaspersky Security for Mobile można znaleźć w *pomocy do Kaspersky Security for Mobile*.

Scenariusz: Wdrażanie Zarządzania urządzeniami mobilnymi

Ta sekcja zawiera scenariusz konfigurowania funkcji Zarządzanie urządzeniami mobilnymi w Kaspersky Security Center.

Wymagania wstępne

Upewnij się, że masz licencję, która daje dostęp do funkcji Zarządzanie urządzeniami mobilnymi.

Etapy

Wdrożenie funkcji Zarządzanie urządzeniami mobilnymi odbywa się w etapach:

1. **Przygotowywanie portów**

   Upewnij się, że port 13292 jest dostępny na Serwerze administracyjnym. Ten port jest wymagany do podłączania urządzeń mobilnych. Możesz także chcieć udostępnić port 17100. Ten port jest wymagany tylko do aktywacji poprzez serwer proxy dla zarządzanych urządzeń mobilnych; jeśli zarządzane urządzenia mobilne mają dostęp do internetu, nie musisz udostępniać tego portu.

2. **Włączanie Zarządzania urządzeniami mobilnymi**

   Możesz włączyć Zarządzanie urządzeniami mobilnymi, gdy uruchamiasz Kreator wstępnej konfiguracji Serwera administracyjnego lub w późniejszym czasie.

3. **Określanie zewnętrznego adresu Serwera administracyjnego**

   Możesz określić zewnętrzny adres, gdy uruchamiasz Kreator wstępnej konfiguracji Serwera administracyjnego lub w późniejszym czasie. Jeśli nie wybrałeś Zarządzania urządzeniami mobilnymi do zainstalowania i nie określiłeś adresu kreatora instalacji, określ zewnętrzny adres we właściwościach pakietu instalacyjnego.

4. **Dodawanie urządzeń mobilnych do grupy Zarządzane urządzenia**

   Dodaj urządzenia mobilne do grupy Zarządzane urządzenia, abyś mógł zarządzać tymi urządzeniami poprzez profile. Możesz utworzyć regułę przenoszenia w jednym z kroków kreatora wstępnej konfiguracji Serwera administracyjnego. Możesz także utworzyć regułę przenoszenia w późniejszym czasie. Jeśli nie utworzysz takiej reguły, możesz ręcznie dodać urządzenia mobilne do grupy Zarządzane urządzenia.

   Możesz dodać urządzenia mobilne bezpośrednio do grupy Zarządzane urządzenia lub możesz utworzyć dla nich podgrupę (lub kilka podgrup).

   W dowolnym późniejszym czasie możesz podłączyć dowolne nowe urządzenie mobilne do Serwera administracyjnego przy użyciu kreatora podłączania nowego urządzenia mobilnego.

5. **Tworzenie profilu dla urządzeń mobilnych**

   Aby zarządzać urządzeniami mobilnymi, utwórz dla nich zasadę (lub kilka zasad) w grupie, do której należą te urządzenia. Możesz zmienić ustawienia tego profilu w dowolnym późniejszym czasie.

Wyniki

Po zakończeniu tego scenariusza, możesz zarządzać urządzeniami Android i iOS przy użyciu Kaspersky Security Center. Możesz pracować z certyfikatami urządzeń mobilnych i wysłać polecenia do urządzeń mobilnych.

Informacje o profilu grupowym do zarządzania urządzeniami EAS i iOS MDM

Aby zarządzać urządzeniami iOS MDM i EAS, możesz wykorzystać wtyczkę zarządzającą Kaspersky Device Management for iOS, która znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Kaspersky Device Management for iOS umożliwia tworzenie zasad grupy do określania ustawień konfiguracji urządzeń iOS MDM i EAS bez użycia narzędzia iPhone® Configuration Utility oraz profilu zarządzającego Exchange ActiveSync.

Profil grupowy do zarządzania urządzeniami EAS i iOS MDM oferuje administratorowi następujące opcje:

- Podczas zarządzania urządzeniami EAS:
    - Konfigurowanie hasła odblokowywania urządzenia.
    - Konfigurowanie przechowywania danych na urządzeniu w postaci zaszyfrowanej.
    - Konfigurowanie synchronizacji poczty firmowej.
    - Konfigurowanie funkcji sprzętowych urządzeń mobilnych, takich jak użycie nośników wymiennych, aparatu lub funkcji Bluetooth.
    - Konfigurowanie ograniczeń korzystania z aplikacji mobilnych na urządzeniu.
- Podczas zarządzania urządzeniami iOS MDM:
    - Konfigurowanie ustawień bezpieczeństwa hasła.
    - Konfigurowanie ograniczeń użycia funkcji sprzętowych urządzenia oraz ograniczeń instalacji i dezinstalacji aplikacji mobilnych.
    - Konfigurowanie ograniczeń użycia fabrycznie zainstalowanych aplikacji mobilnych, takich jak YouTube™, iTunes® Store lub Safari.
    - Konfigurowanie ograniczeń przeglądania mediów (filmów i programów TV) według regionu, w którym zlokalizowane jest urządzenie.
    - Konfigurowanie ustawień połączenia urządzenia z internetem poprzez serwer proxy (globalny serwer pośredniczący HTTP).
    - Konfigurowanie ustawień konta, przy użyciu którego użytkownik może uzyskać dostęp do usług i aplikacji firmowych (technologia pojedynczego logowania - Single Sign On).
    - Monitorowanie korzystania z internetu (odwiedzanych stron internetowych) na urządzeniach mobilnych.
    - Konfigurowanie ustawień sieci bezprzewodowych (Wi-Fi), punktów dostępu (APN) i wirtualnych sieci prywatnych (VPN), które używają różnych mechanizmów autoryzacji i protokołów sieciowych.
    - Konfigurowanie ustawień nawiązywania połączenia z urządzeniami AirPlay® do przesyłania zdjęć, muzyki i filmów.
    - Konfigurowanie ustawień nawiązywania połączenia z drukarkami AirPrint™ w celu bezprzewodowego drukowania dokumentów z urządzenia.
    - Konfigurowanie ustawień synchronizacji z serwerem Microsoft Exchange i kontami użytkowników w celu korzystania z poczty firmowej na urządzeniach.
    - Konfigurowanie danych uwierzytelniających użytkowników do synchronizacji z usługą katalogową LDAP.
    - Konfigurowanie danych uwierzytelniających użytkowników do nawiązywania połączenia z usługami CalDAV i CardDAV, które dają użytkownikom dostęp do kalendarzy firmowych i list kontaktów.
    - Konfigurowanie ustawień interfejsu iOS na urządzeniu użytkownika, takich jak czcionki lub ikony dla ulubionych stron internetowych.
    - Dodawanie nowych certyfikatów zabezpieczeń na urządzeniach.

- Konfigurowanie ustawień serwera Simple Certificate Enrollment Protocol (SCEP) do automatycznego pobierania certyfikatów z Urzędu certyfikacji.

- Dodawanie niestandardowych ustawień dla pracy z aplikacjami mobilnymi.

Profil do zarządzania urządzeniami EAS i iOS MDM wyróżnia się tym, że jest przypisany do grupy administracyjnej, która zawiera serwer iOS MDM oraz serwer urządzeń mobilnych Exchange ActiveSync (zwane dalej "serwery urządzeń mobilnych"). Wszystkie ustawienia określone w tym profilu są w pierwszej kolejności stosowane do serwerów urządzeń mobilnych, a następnie do urządzeń mobilnych zarządzanych przez takie serwery. W przypadku hierarchicznej struktury grup administracyjnych, podrzędne serwery urządzeń mobilnych pobierają ustawienia zasady z głównych serwerów urządzeń mobilnych i rozsyłają je na urządzenia mobilne.

Więcej informacji dotyczących używania zasady grupowej do zarządzania urządzeniami EAS i iOS MDM w Konsoli administracyjnej Kaspersky Security Center można znaleźć w dokumentacji do *Kaspersky Security for Mobile*.

Włączanie Zarządzania urządzeniami mobilnymi

Aby możliwe było zarządzanie urządzeniami mobilnymi, należy włączyć Zarządzanie urządzeniami mobilnymi. Jeśli nie włączono tej funkcji w kreatorze wstępnej konfiguracji, możesz włączyć ją później. Zarządzanie urządzeniami mobilnymi wymaga licencji.

Włączenie Zarządzania urządzeniami mobilnymi jest dostępne tylko na głównym Serwerze administracyjnym.

W celu włączenia Zarządzania urządzeniami mobilnymi:

1. W drzewie konsoli wybierz folder **Zarządzanie urządzeniami mobilnymi**.

2. W obszarze roboczym folderu kliknij przycisk **Włącz zarządzanie urządzeniami mobilnymi**. Ten przycisk jest dostępny, jeśli wcześniej nie włączyłeś **Zarządzanie urządzeniami mobilnymi**.

   Zostanie wyświetlone okno **Dodatkowe składniki** kreatora wstępnej konfiguracji Serwera administracyjnego.

3. Wybierz **Włącz zarządzanie urządzeniami mobilnymi**, aby zarządzać urządzeniami mobilnymi.

4. W oknie **Wybierz metodę aktywacji aplikacji** aktywuj aplikację przy użyciu pliku klucza lub kodu aktywacyjnego.

   Zarządzanie urządzeniami mobilnymi będzie niemożliwe, dopóki nie aktywujesz funkcji Zarządzanie urządzeniami mobilnymi.

5. Na stronie **Ustawienia serwera proxy umożliwiającego dostęp do internetu** zaznacz pole **Użyj serwera proxy**, jeśli podczas nawiązywania połączenia z internetem chcesz używać serwera proxy. Jeśli to pole jest zaznaczone, dostępne staną się pola do wprowadzenia ustawień. Określ ustawienia połączenia z serwerem proxy.

6. Na stronie **Sprawdzanie aktualizacji dla wtyczek i pakietów instalacyjnych** wybierz jedną z następujących opcji:

   - **Sprawdź, czy wtyczki i pakiety instalacyjne są aktualne**

     Rozpoczynanie sprawdzania, czy wtyczki i pakiety instalacyjne są aktualne. Jeśli podczas sprawdzania zostaną wykryte przestarzałe wersje wtyczek lub pakietów instalacyjnych, kreator wyświetli okno z pytaniem o pobranie aktualnych wersji do zastąpienia tych przestarzałych.

   - **Pomiń sprawdzanie**

Kontynuowanie pracy bez sprawdzania, czy wtyczki i pakiety instalacyjne są aktualne. Możesz wybrać tę opcję, jeśli, na przykład, nie posiadasz dostępu do Internetu lub jeśli z jakiegoś powodu chcesz korzystać z przestarzałej wersji aplikacji.

Pominięcie sprawdzania dostępności uaktualnień dla wtyczek może spowodować niepoprawne działanie aplikacji.

7. W oknie **Dostępna jest najnowsza wersja wtyczki** pobierz i zainstaluj najnowsze wersje wtyczek w wersji językowej wymaganej przez wersję posiadanej aplikacji. Do aktualizowania wtyczek nie jest wymagana licencja.

   Po zainstalowaniu wtyczek i pakietów, aplikacja sprawdza, czy zainstalowane są wszystkie wtyczki niezbędne do poprawnego działania urządzeń mobilnych. Jeśli zostaną wykryte przestarzałe wersje wtyczek, kreator wyświetli okno z pytaniem o pobranie aktualnych wersji do zastąpienia tych przestarzałych.

8. Na stronie **Ustawienia połączenia urządzenia mobilnego** skonfiguruj porty Serwera administracyjnego.

Po zakończeniu pracy kreatora zostaną wprowadzone następujące zmiany:

- Zostanie utworzony profil Kaspersky Endpoint Security for Android.
- Zostanie utworzony profil Kaspersky Device Management for iOS.
- Porty zostaną otwarte na Serwerze administracyjnym dla urządzeń mobilnych.

Modyfikowanie ustawień Zarządzania urządzeniami mobilnymi

W celu włączenia obsługi urządzeń mobilnych:

1. W drzewie konsoli wybierz folder **Zarządzanie urządzeniami mobilnymi**.
2. W obszarze roboczym folderu kliknij odnośnik **Porty połączenia dla urządzeń mobilnych**.

   Zostanie wyświetlona sekcja **Porty dodatkowe** okna właściwości Serwera administracyjnego.
3. W sekcji **Porty dodatkowe** zmodyfikuj odpowiednie ustawienia:

   - **Port SSL do aktywacji przy użyciu serwera proxy**

     Numer portu SSL do połączenia Kaspersky Endpoint Security for Windows z serwerami aktywacji Kaspersky.

     Domyślny numer portu to 17000.

   - **Otwórz port dla urządzeń mobilnych**

     Port zostaje otwarty dla urządzeń mobilnych do połączenia z serwerem licencjonowania. Możesz zdefiniować numer portu i inne ustawienia w polach poniżej.

     Domyślnie opcja ta jest włączona.

   - **Port do synchronizacji urządzeń mobilnych**

Numer portu, za pomocą którego urządzenia mobilne będą łączyć się z Serwerem administracyjnym i będą wymieniać z nim dane. Domyślny numer portu to 13292.

Jeśli port 13292 jest używany do innych celów, można przypisać inny port.

- Port do aktywacji urządzeń mobilnych

  Port do łączenia Kaspersky Endpoint Security for Android z serwerami aktywacji Kaspersky.

  Domyślny numer portu to 17100.

4. Kliknij **OK**.

Wyłączanie Zarządzania urządzeniami mobilnymi

Wyłączenie Zarządzania urządzeniami mobilnymi jest dostępne tylko na głównym Serwerze administracyjnym.

W celu wyłączenia Zarządzania urządzeniami mobilnymi:

1. W drzewie konsoli wybierz folder **Zarządzanie urządzeniami mobilnymi**.
2. W obszarze roboczym tego folderu kliknij odnośnik **Skonfiguruj dodatkowe składniki**.

   Zostanie wyświetlone okno **Dodatkowe składniki** kreatora wstępnej konfiguracji Serwera administracyjnego.
3. Wybierz **Nie włączaj Zarządzania urządzeniami mobilnymi**, jeśli nie chcesz już zarządzać urządzeniami mobilnymi.
4. Kliknij **OK**.

Wcześniej podłączone urządzenia mobilne nie będą mogły nawiązać połączenia z Serwerem administracyjnym. Port dla połączenia urządzenia mobilnego oraz port dla aktywacji urządzenia mobilnego zostaną zamknięte automatycznie.

Profile, które zostały utworzone dla Kaspersky Endpoint Security for Android i Kaspersky Device Management for iOS, nie zostaną usunięte. Reguły wydawania certyfikatów nie zostaną zmodyfikowane. Zainstalowane wtyczki nie zostaną usunięte. Reguła przenoszenia dla urządzeń mobilnych nie zostanie usunięta.

Po ponownym włączeniu Zarządzania urządzeniami mobilnymi na zarządzanych urządzeniach mobilnych, konieczne może być ponowne zainstalowanie aplikacji mobilnych, wymaganych do zarządzania urządzeniami mobilnymi.

Praca z poleceniami dla urządzeń mobilnych

Ta sekcja zawiera informacje o poleceniach do zarządzania urządzeniami mobilnymi obsługiwanych przez aplikację. Sekcja zawiera instrukcje dotyczące wysyłania poleceń na urządzenia mobilne, a także dotyczące przeglądania stanów wykonywania poleceń w raporcie poleceń.

Polecenia zarządzania urządzeniem mobilnym

Kaspersky Security Center obsługuje polecenia do zarządzania urządzeniami mobilnymi.

Takie polecenia są używane do zdalnego zarządzania urządzeniami mobilnymi. Na przykład, gdy urządzenie mobilne zostanie zgubione, można usunąć z niego wszystkie dane firmowe, korzystając z odpowiedniego polecenia.

Możesz użyć poleceń dla następujących typów zarządzanych urządzeń mobilnych:

- Urządzenia iOS MDM
- Urządzenia Kaspersky Endpoint Security (KES)
- Urządzenia EAS

Każde urządzenie obsługuje dedykowany zestaw poleceń.

Uwagi dotyczące pewnych poleceń

- W przypadku wszystkich typów urządzeń, gdy polecenie **Przywróć ustawienia fabryczne** zostanie pomyślnie wykonane, wszystkie dane zostaną usunięte z urządzenia i zostaną przywrócone ustawienia fabryczne.
- Po pomyślnym wykonaniu polecenia **Wyczyść dane firmowe** na urządzeniu iOS MDM, wszystkie zainstalowane profile konfiguracyjne, profile informacyjne, profil iOS MDM oraz aplikacje, dla których zaznaczono pole **Usuń wraz z profilem iOS MDM**, zostaną usunięte z urządzenia.
- Jeśli polecenie **Wyczyść dane firmowe** zostanie pomyślnie wykonane na urządzeniu KES, wszystkie dane firmowe, wpisy z Kontaktów, historia wiadomości SMS, rejestr połączeń, kalendarz, ustawienia połączenia internetowego oraz konta użytkownika (za wyjątkiem konta Google™) zostaną usunięte z urządzenia. W przypadku urządzeń KES zostaną usunięte także wszystkie dane z karty pamięci.
- Przed wysłaniem polecenia **Lokalizacja** na urządzenie KES konieczne będzie potwierdzenie, że korzystasz z tego polecenia do autoryzowanego wyszukiwania zagubionego urządzenia, które należy do Twojej organizacji lub do jednego z pracowników. Urządzenie mobilne, które otrzymuje polecenie **Lokalizacja**, nie jest zablokowane.

Lista poleceń dla urządzeń mobilnych

Poniższa tabela wyświetla zestawy poleceń dla urządzeń iOS MDM.

Obsługiwane polecenia do zarządzania urządzeniami mobilnymi: urządzenia iOS MDM

Polecenia	Wynik wykonania polecenia
Zablokuj	Urządzenie mobilne zostanie zablokowane.
Odblokuj	Zablokowanie urządzenia mobilnego przy użyciu kodu PIN jest wyłączone. Wcześniej określony kod PIN został zresetowany.
Przywróć ustawienia fabryczne	Wszystkie dane zostaną usunięte z urządzenia mobilnego oraz zostaną przywrócone ustawienia domyślne.
Wyczyść dane firmowe	Wszystkie zainstalowane profile konfiguracyjne, profile informacyjne, profil iOS MDM oraz aplikacje, dla których zaznaczono pole **Usuń wraz z profilem iOS MDM**, zostaną usunięte z urządzenia.

Synchronizuj urządzenie	Dane urządzenia mobilnego zostaną zsynchronizowane z Serwerem administracyjnym.
Zainstaluj profil	Profil konfiguracyjny zostaje zainstalowany na urządzeniu mobilnym.
Usuń profil	Profil konfiguracyjny zostaje usunięty z urządzenia mobilnego.
Zainstaluj profil informacyjny	Profil informacyjny zostaje zainstalowany na urządzeniu mobilnym.
Usuń profil informacyjny	Profil informacyjny zostaje usunięty z urządzenia mobilnego.
Zainstaluj aplikację	Aplikacja zostanie zainstalowana na urządzeniu mobilnym.
Usuń aplikację	Aplikacja zostanie usunięta z urządzenia mobilnego.
Wprowadź kod wykupu	Wprowadzenie kodu wykupu dla płatnej aplikacji.
Konfiguruj roaming	Włączenie lub wyłączenie roamingu danych i roamingu połączeń.

Poniższa tabela wyświetla zestawy poleceń dla urządzeń KES.

Obsługiwane polecenia zarządzania urządzeniami mobilnymi: urządzenia KES

Polecenie	Wynik wykonania polecenia
Zablokuj	Urządzenie mobilne zostanie zablokowane.
Odblokuj	Zablokowanie urządzenia mobilnego przy użyciu kodu PIN jest wyłączone. Wcześniej określony kod PIN został zresetowany.
Przywróć ustawienia fabryczne	Wszystkie dane zostaną usunięte z urządzenia mobilnego oraz zostaną przywrócone ustawienia domyślne.
Wyczyść dane firmowe	Dane firmowe, wpisy w Kontaktach, historia wiadomości SMS, rejestr połączeń, kalendarz, ustawienia połączenia internetowego oraz konta użytkownika (za wyjątkiem konta Google) zostaną usunięte. Dane znajdujące się na karcie pamięci także zostaną usunięte.
Synchronizuj urządzenie	Dane urządzenia mobilnego zostaną zsynchronizowane z Serwerem administracyjnym.
Zlokalizuj urządzenie	Urządzenie mobilne zostanie zlokalizowanie, a jego pozycja zostanie wyświetlona na Google Maps™. Operator telefonii komórkowej pobiera opłatę za wysłanie wiadomości SMS oraz za korzystanie z internetu.
Wykonaj zdjęcie (mugshot)	Urządzenie mobilne zostanie zablokowane. Zostanie wykonane zdjęcie urządzenia przednią kamerą, a następnie zostanie ono wysłane na Serwer administracyjny. Zdjęcia można przejrzeć w raporcie poleceń. Operator telefonii komórkowej pobiera opłatę za wysłanie wiadomości SMS oraz za korzystanie z internetu.
Alarm	Urządzenie mobilne włączy alarm.

Poniższa tabela wyświetla polecenia dla urządzeń EAS.

Obsługiwane polecenia zarządzania urządzeniami mobilnymi: urządzenia KES

Polecenia	Wynik wykonania polecenia
Przywróć ustawienia	Wszystkie dane zostaną usunięte z urządzenia mobilnego oraz zostaną

fabryczne	przywrócone ustawienia domyślne.

Korzystanie z Google Firebase Cloud Messaging

Aby zapewnić dostarczanie w odpowiednim momencie poleceń na urządzenia KES działające pod systemem operacyjnym Android, Kaspersky Security Center korzysta z mechanizmów powiadomień push. Powiadomienia push są wymieniane między urządzeniami KES a Serwerem administracyjnym poprzez Google Firebase Cloud Messaging. W Konsoli administracyjnej Kaspersky Security Center możesz określić ustawienia Google Firebase Cloud Messaging do podłączania urządzeń KES do usługi.

Aby pobrać ustawienia Google Firebase Cloud Messaging, należy posiadać konto Google.

W celu skonfigurowania Google Firebase Cloud Messaging:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.
2. Z otwartego menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.

   Zostanie otwarte okno właściwości folderu **Urządzenia mobilne**.
3. Wybierz sekcję **Ustawienia Google Firebase Cloud Messaging**.
4. W polu **ID nadawcy** określ numer projektu Google API, który otrzymałeś podczas tworzenia go w konsoli Google Developer Console.
5. W polu **Klucz serwera** wprowadź standardowy klucz serwera, który utworzyłeś w konsoli Google Developer Console.

Przy kolejnej synchronizacji z Serwerem administracyjnym, urządzenia KES, działające pod systemami operacyjnymi Android, zostaną połączone z Google Firebase Cloud Messaging.

Możesz zmodyfikować ustawienia Google Firebase Cloud Messaging, klikając przycisk **Resetuj ustawienia**.

Wysyłanie poleceń

W celu wysłania polecenia na urządzenie mobilne użytkownika:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.
2. Wybierz urządzenie mobilne użytkownika, na które chcesz wysłać polecenie.
3. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.
4. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji z nazwą polecenia, które chcesz wysłać na urządzenie mobilne, a następnie kliknij przycisk **Wyślij polecenie**.

   W zależności od wybranego polecenia, kliknięcie przycisku **Wyślij polecenie** może spowodować otwarcie okna zaawansowanych ustawień aplikacji. Na przykład, jeśli wyślesz polecenie usunięcia profilu informacyjnego z urządzenia mobilnego, aplikacja wyświetli pytanie o wybór profilu informacyjnego, który musi zostać usunięty z urządzenia mobilnego. Zdefiniuj zaawansowane ustawienia polecenia w tym oknie i potwierdź swój wybór. Polecenie zostanie wysłane na urządzenie mobilne.

Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

5. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Przeglądanie stanów poleceń w raporcie poleceń

Aplikacja zapisuje do raportu poleceń informacje o wszystkich poleceniach, które zostały wysłane na urządzenia mobilne. Raport poleceń zawiera informacje o godzinie i dacie wysłania każdego polecenia na urządzenie mobilne, ich odpowiednich stanach i szczegółowych opisach wyników wykonania poleceń. Na przykład, gdy wykonanie polecenia zakończy się niepowodzeniem, raport będzie wyświetlał przyczynę błędu. Wpisy są przechowywane w raporcie poleceń najwyżej przez 30 dni.

Polecenia wysłane na urządzenia mobilne mogą posiadać następujące stany:

- *Uruchomione*—polecenie zostało wysłane na urządzenie mobilne.
- *Zakończone*—wykonanie polecenia zostało pomyślnie zakończone.
- *Zakończone błędem*—wykonanie polecenia nie powiodło się.
- *Usuwanie*— polecenie jest usuwane z kolejki poleceń wysyłanych na urządzenie mobilne.
- *Usunięte*—polecenie zostało usunięte z kolejki poleceń wysyłanych na urządzenie mobilne.
- *Błąd usuwania*—polecenie nie mogło zostać usunięte z kolejki poleceń wysyłanych na urządzenie mobilne.

Aplikacja przechowuje raport poleceń dla każdego urządzenia mobilnego.

W celu przejrzenia raportu poleceń wysłanych na urządzenie mobilne:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. Na liście urządzeń mobilnych wybierz to, dla którego chcesz przejrzeć raport poleceń.

3. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

   Zostanie otwarte okno **Polecenia administracyjne urządzenia mobilnego**. Sekcje okna **Polecenia administracyjne urządzenia mobilnego** odpowiadają poleceniom, które mogą być wysłane na urządzenie mobilne.

4. Wybierz sekcje zawierające żądane polecenia i przejrzyj informacje dotyczące wysłania i wykonania poleceń w sekcji **Raport poleceń**.

W sekcji **Raport poleceń** możesz przejrzeć listę poleceń, które zostały wysłane na urządzenie mobilne, oraz szczegóły dotyczące tych poleceń. Filtr **Pokaż polecenia** umożliwia wyświetlanie na liście tylko poleceń z wybranym stanem.

Praca z certyfikatami urządzeń mobilnych

Ta sekcja zawiera informacje dotyczące pracy z certyfikatami urządzeń mobilnych. Można tu także znaleźć instrukcje dotyczące instalacji certyfikatów na urządzeniach mobilnych użytkowników oraz konfiguracji reguł wydawania certyfikatów. W sekcji znajdują się również instrukcje dotyczące integracji aplikacji z infrastrukturą publicznych kluczy oraz konfiguracji obsługi Kerberosa (system autoryzacji).

Uruchamianie kreatora instalacji certyfikatu

Na urządzeniu mobilnym użytkownika możesz zainstalować następujące typy certyfikatów:

- Certyfikaty współdzielone do identyfikacji urządzenia mobilnego
- Certyfikat pocztowy do konfiguracji poczty firmowej na urządzeniu mobilnym
- Certyfikat VPN do konfigurowania dostępu do wirtualnej sieci prywatnej na urządzeniu mobilnym

W celu zainstalowania certyfikatu na urządzeniu mobilnym użytkownika:

1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.
2. W obszarze roboczym folderu **Certyfikaty** kliknij odnośnik **Dodaj certyfikat**, aby uruchomić kreator instalacji certyfikatu.

Postępuj zgodnie z instrukcjami kreatora.

Po zakończeniu działania kreatora, certyfikat zostanie utworzony i dodany do listy certyfikatów użytkownika. Dodatkowo, do użytkownika zostanie wysłane powiadomienie zawierające odsyłacz do pobrania i zainstalowania certyfikatu na urządzeniu mobilnym. Listę wszystkich certyfikatów można przejrzeć oraz wyeksportować do pliku. Możesz usunąć i ponownie wydać certyfikaty, a także wyświetlić ich właściwości.

Krok 1. Wybieranie typu certyfikatu

Określ typ certyfikatu, który musi być zainstalowany na urządzeniu mobilnym użytkownika:

- **Certyfikat dla urządzeń mobilnych**—do identyfikowania urządzenia mobilnego
- **Certyfikat pocztowy**—do skonfigurowania poczty firmowej na urządzeniu mobilnym
- **Certyfikat VPN**—do skonfigurowania dostępu do wirtualnej sieci prywatnej na urządzeniu mobilnym

Krok 2. Wybieranie typu urządzenia

To okno jest wyświetlane tylko wtedy, gdy jako typ certyfikatu wybrałeś **Certyfikat pocztowy** lub **Certyfikat VPN**.

Określ typ systemu operacyjnego na urządzeniu:

- **Urządzenie iOS MDM**. Wybierz tę opcję, jeśli musisz zainstalować certyfikat na urządzeniu mobilnym, które jest podłączone do serwera iOS MDM przy użyciu protokołu iOS MDM.
- **Urządzenie KES zarządzane przez Kaspersky Security for Mobile**. Wybierz tę opcję, jeśli musisz zainstalować certyfikat na urządzeniu KES. W tym przypadku certyfikat będzie używany do identyfikacji użytkownika po każdym połączeniu z Serwerem administracyjnym.
- **Urządzenie KES połączone z Serwerem administracyjnym bez uwierzytelniania certyfikatu użytkownika**. Wybierz tę opcję, jeśli musisz zainstalować certyfikat na urządzeniu KES bez użycia uwierzytelniania certyfikatu. W tym przypadku, w ostatnim kroku kreatora, w oknie **Metoda powiadamiania użytkownika** administrator musi wybrać typ uwierzytelniania użytkownika używany przy każdym połączeniu z Serwerem administracyjnym.

Krok 3. Wybieranie użytkownika

Na liście wybierz użytkowników, grupy użytkowników lub grupy użytkowników Active Directory, dla których musisz zainstalować certyfikat.

W oknie **Wybór użytkownika** możesz wyszukać użytkowników wewnętrznych Kaspersky Security Center. Możesz kliknąć **Dodaj**, aby dodać użytkownika wewnętrznego.

Krok 4. Wybieranie źródła certyfikatu

W tym oknie można wybrać źródło certyfikatu, którego Serwer administracyjny będzie używał do identyfikowania urządzeń mobilnych. Certyfikat można określić przy użyciu jednej z następujących metod:

- Automatycznie utwórz certyfikat przy użyciu narzędzi Serwera administracyjnego, a następnie wyślij certyfikat na urządzenie.
- Określ plik certyfikatu, który został utworzony wcześniej. Ta metoda nie jest dostępna, jeśli w poprzednim kroku zaznaczono wielu użytkowników.

Zaznacz pole **Opublikuj certyfikat**, jeśli musisz wysłać użytkownikowi powiadomienie o utworzeniu certyfikatu dla jego/jej urządzenia mobilnego.

Jeśli dla urządzenia mobilnego użytkownika przeprowadzono już uwierzytelnianie z użyciem certyfikatu, dzięki czemu nie ma potrzeby określenia nazwy konta i hasła do pobrania nowego certyfikatu, odznacz pole **Opublikuj certyfikat**. W tym przypadku okno **Metoda powiadamiania użytkownika** nie zostanie wyświetlone.

Krok 5. Przypisywanie znacznika do certyfikatu

Okno **Znacznik certyfikatu** jest wyświetlane, jeśli opcja **Urządzenie iOS MDM** została wybrana w **Typ urządzenia**.

Na liście rozwijalnej możesz przypisać znacznik do certyfikatu urządzenia iOS MDM użytkownika. Certyfikat z przypisanym znacznikiem może posiadać określone parametry ustawione dla tego znacznika we właściwościach zasady Kaspersky Device Management for iOS.

Lista rozwijana oferuje wybranie znacznika *Szablon certyfikatu 1*, *Szablon certyfikatu 2* lub *Szablon certyfikatu 3*. Znaczniki można skonfigurować w następujących sekcjach:

- Jeśli w oknie **Typ certyfikatu** wybrano **Certyfikat pocztowy**, znaczniki dla tego certyfikatu można skonfigurować we właściwościach konta Exchange ActiveSync dla urządzeń mobilnych (**Zarządzane urządzenia** → **Zasady** → Właściwości zasady Kaspersky Device Management for iOS > sekcja **Exchange ActiveSync** → **Dodaj** → **Zaawansowane**).

- Jeśli w oknie **Typ certyfikatu** wybrano **Certyfikat VPN**, znaczniki dla tego certyfikatu można skonfigurować we właściwościach VPN dla urządzeń mobilnych (**Zarządzane urządzenia** → **Zasady** → Właściwości zasady Kaspersky Device Management for iOS → sekcja **VPN** → **Dodaj** → **Zaawansowane**). Nie możesz skonfigurować znaczników używanych dla certyfikatów VPN, jeśli dla swojego VPN wybrano typ połączenia L2TP, PPTP lub IPSec (Cisco™).

Krok 6. Określanie ustawień publikowania certyfikatu

W tym oknie możesz określić następujące ustawienia publikowania certyfikatu:

- **Nie powiadamiaj użytkownika o nowym certyfikacie**

  Włącz tę opcję, jeśli nie chcesz wysłać użytkownikowi powiadomienia o tworzeniu certyfikatu dla urządzenia mobilnego użytkownika. W tym przypadku okno **Metoda powiadamiania użytkownika** nie zostanie wyświetlone.

  > Ta opcja jest stosowana tylko do urządzeń z zainstalowanym programem Kaspersky Endpoint Security for Android.

  Możesz włączyć tę opcję, na przykład, jeśli urządzenie mobilne użytkownika zostało wcześniej uwierzytelnione przy użyciu certyfikatu, więc nie ma konieczności określenia nazwy konta i hasła do odebrania nowego certyfikatu.

- **Zezwól urządzeniu na wielu odbiorców jednego certyfikatu (wyłącznie dla urządzeń z zainstalowaną aplikacją Kaspersky Endpoint Security for Android)**

  Włącz tę opcję, jeśli chcesz, żeby Kaspersky Security Center automatycznie rozsyłała certyfikat za każdym razem, gdy wkrótce wygaśnie lub gdy nie zostanie znaleziony na urządzeniu docelowym.

  Certyfikat jest automatycznie rozsyłany kilka dni przed datą wygaśnięcia certyfikatu. Możesz ustawić liczbę dni w oknie Reguły wydawania certyfikatu.

  W niektórych przypadkach certyfikat nie może zostać znaleziony na urządzeniu. Na przykład, to może mieć miejsce, gdy użytkownik zainstaluje ponownie aplikację zabezpieczającą Kaspersky na urządzeniu lub zresetuje dane i przywróci domyślne ustawienia urządzenia. W tym przypadku Kaspersky Security Center sprawdza identyfikator urządzenia przy kolejnej próbie połączenia urządzenia z Serwerem administracyjnym. Jeśli urządzenie posiada ten sam identyfikator, który miał, gdy certyfikat został wydany, aplikacja wyśle certyfikat na urządzenie.

Krok 7. Wybieranie metody powiadamiania użytkownika

To okno nie jest wyświetlane, jeśli jako typ urządzenia wybrałeś **Urządzenie iOS MDM** lub jeśli wybrałeś opcję **Nie powiadamiaj użytkownika o nowym certyfikacie**.

W sekcji **Metoda powiadamiania użytkownika** możesz skonfigurować powiadamianie użytkownika o instalacji certyfikatu na urządzeniu mobilnym.

W polu **Metoda uwierzytelniania** określ typ uwierzytelniania użytkownika:

- **Poświadczenia (domena lub alias)**

  W tym przypadku, do pobrania nowego certyfikatu użytkownik stosuje hasło domeny lub hasło wewnętrznego użytkownika Kaspersky Security Center.

- **Hasło jednorazowe**

  W tym przypadku użytkownik otrzymuje hasło jednorazowe, które zostanie wysłane w wiadomości e-mail lub SMS. To hasło musi zostać wprowadzone, aby możliwe było pobranie nowego certyfikatu.

  Ta opcja zmieni się na **Hasło**, jeśli w oknie **Ustawienia publikowania certyfikatu** włączyłeś (zaznaczyłeś) opcję **Zezwól na wiele urządzeń odbierających jeden certyfikat (wyłącznie dla urządzeń mobilnych z zainstalowanymi aplikacjami Kaspersky)**.

- **Hasło**

  W tym przypadku hasło jest używane za każdym razem, gdy certyfikat zostanie wysłany do użytkownika.

  Ta opcja zmieni się na **Hasło jednorazowe**, jeśli w oknie **Ustawienia publikowania certyfikatu** wyłączyłeś (odznaczyłeś) opcję **Zezwól na wiele urządzeń odbierających jeden certyfikat (wyłącznie dla urządzeń mobilnych z zainstalowanymi aplikacjami Kaspersky)**.

To pole jest wyświetlane, jeśli wybrałeś **Certyfikat dla urządzeń mobilnych** w oknie **Typ certyfikatu** lub jeśli jako typ urządzenia wybrałeś **Urządzenie KES połączone z Serwerem administracyjnym bez uwierzytelniania certyfikatu użytkownika**.

Wybierz opcję powiadamiania użytkownika:

- **Po zakończeniu działania kreatora wyświetl hasło uwierzytelniające**

Jeśli wybierzesz tę opcję, nazwa użytkownika, nazwa użytkownika w Menedżerze kont zabezpieczeń (SAM), a także hasło do odzyskania certyfikatu dla każdego z wybranych użytkowników zostanie wyświetlone w ostatnim kroku kreatora instalacji certyfikatu. Konfiguracja powiadamiania użytkownika o zainstalowanym certyfikacie będzie niedostępna.

Jeśli dodasz certyfikaty dla kilku użytkowników, możesz zapisać dostarczone poświadczenia do pliku, klikając przycisk **Eksportuj** w ostatnim kroku kreatora instalacji certyfikatu.

Ta opcja jest niedostępna, jeśli w kroku **Metoda powiadamiania użytkownika** wybrano Poświadczenia (domena lub alias).

- **Powiadom użytkownika o nowym certyfikacie**

  Jeśli wybierzesz tę opcję, możesz skonfigurować powiadamianie użytkownika o nowym certyfikacie.

  - **Przez e-mail**

    W tej grupie ustawień możesz skonfigurować powiadamianie użytkownika o instalacji nowego certyfikatu na jego urządzeniu mobilnym za pośrednictwem wiadomości e-mail. Ta metoda powiadamiania jest dostępna tylko wtedy, gdy opcja Serwer SMTP jest włączona.

    Kliknij odnośnik **Edytuj wiadomość**, aby wyświetlić i edytować powiadomienie (jeśli to konieczne).

  - **Przez SMS**

    W tej grupie ustawień możesz skonfigurować powiadamianie użytkownika o używaniu wiadomości SMS do zainstalowania certyfikatu na urządzeniach mobilnych. Ta metoda powiadamiania jest dostępna tylko wtedy, gdy opcja Powiadomienia SMS jest włączona.

    Kliknij odnośnik **Edytuj wiadomość**, aby wyświetlić i edytować powiadomienie (jeśli to konieczne).

Krok 8. Generowanie certyfikatu

W tym kroku zostanie utworzony certyfikat.

Możesz kliknąć **Zakończ**, aby zakończyć działanie kreatora.

Certyfikat zostanie wygenerowany i wyświetlony na liście certyfikatów, w obszarze roboczym folderu **Certyfikaty**.

Konfigurowanie reguł wydawania certyfikatów

Certyfikaty są używane do autoryzacji urządzenia na Serwerze administracyjnym. Wszystkie zarządzane urządzenia mobilne muszą posiadać certyfikaty. Możesz skonfigurować sposób publikowania certyfikatów.

W celu skonfigurowania reguł wydawania certyfikatu:

1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.

2. W obszarze roboczym folderu **Certyfikaty** kliknij przycisk **Konfiguruj reguły wydawania certyfikatów**, aby otworzyć okno **Reguły wydawania certyfikatu**.

3. Przejdź do sekcji z nazwą typu certyfikatu:

   Wydawanie certyfikatów dla urządzeń mobilnych—aby skonfigurować wydawanie certyfikatów dla urządzeń mobilnych.

   Wydawanie certyfikatów pocztowych—aby skonfigurować wydawanie certyfikatów pocztowych.

   Wydawanie certyfikatów VPN—aby skonfigurować wydawanie certyfikatów VPN.

4. W sekcji **Ustawienia wydawania** skonfiguruj wydawanie certyfikatów:

   - Określ czas życia certyfikatu w dniach.
   - Wybierz źródło certyfikatu (**Serwer administracyjny** lub **Certyfikaty określone ręcznie**).

     Serwer administracyjny jest wybrany jako domyślne źródło certyfikatów.
   - Określ szablon certyfikatu (**Szablon domyślny**, **Inny szablon**).

     Konfiguracja szablonów jest dostępna, jeśli sekcja **Integracja z PKI** zawiera włączoną integrację z infrastrukturą kluczy publicznych.

5. W sekcji **Ustawienia aktualizacji automatycznych** skonfiguruj automatyczne aktualizacje certyfikatu:

   - W polu **Odnów, gdy certyfikat wygaśnie za (dni)** określ, ile dni przed wygaśnięciem certyfikat powinien zostać odnowiony.
   - Aby włączyć automatyczne aktualizacje certyfikatów, zaznacz pole **Odnów certyfikat automatycznie, jeśli jest to możliwe**.

   Certyfikat dla urządzeń mobilnych można odnowić tylko ręcznie.

6. W sekcji **Ochrona hasłem** włącz i skonfiguruj użycie hasła podczas deszyfrowania certyfikatów.

   > Ochrona hasłem jest dostępna tylko dla certyfikatów dla urządzeń mobilnych.

   a. Zaznacz pole **Pytaj o hasło podczas instalowania certyfikatów**.

   b. Użyj suwaka, aby zdefiniować maksymalną liczbę znaków w haśle do szyfrowania.

7. Kliknij **OK**.

Integracja z infrastrukturą kluczy publicznych

Integracja aplikacji z Infrastrukturą klucza publicznego (PKI) jest wymagana do uproszczenia wydawania użytkownikom certyfikatów dla domen. Po przeprowadzeniu integracji certyfikaty są generowane automatycznie.

> Minimalna obsługiwana wersja serwera PKI to Windows Server 2008.

Musisz skonfigurować konto do integracji z PKI. Konto musi spełniać następujące wymagania:

- Musi być użytkownikiem domeny i administratorem urządzenia, na którym jest zainstalowany Serwer administracyjny.
- Na urządzeniu z zainstalowanym Serwerem administracyjnym musi mieć nadane uprawnienie SeServiceLogonRight.

Aby utworzyć profil użytkownika na stałe, zaloguj się przynajmniej raz z poziomu skonfigurowanego konta użytkownika na urządzeniu, na którym znajduje się Serwer administracyjny. W repozytorium certyfikatów tego użytkownika na urządzeniu, na którym znajduje się Serwer administracyjny, zainstaluj certyfikat Agenta wycofywania, dostarczony przez administratorów domeny.

W celu skonfigurowania integracji z infrastrukturą kluczy publicznych:

1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.
2. W obszarze roboczym kliknij przycisk **Zintegruj z infrastrukturą klucza publicznego**, aby otworzyć sekcję **Integracja z PKI** okna **Reguły wydawania certyfikatu**.

   Zostanie otwarta sekcja **Integracja z PKI** okna **Reguły wydawania certyfikatu**.
3. Zaznacz pole **Zintegruj wystawianie certyfikatów z PKI**.
4. W polu **Konto** określ nazwę konta użytkownika używanego do integracji z infrastrukturą kluczy publicznych.
5. W polu **Hasło** wprowadź hasło domeny do konta.
6. Z listy **Nazwa szablonu certyfikatu w systemie PKI** wybierz szablon certyfikatu, który zostanie użyty do wydania certyfikatów użytkownikom domeny.

   Dedykowana usługa jest uruchamiana w Kaspersky Security Center z poziomu określonego konta użytkownika. Ta usługa jest odpowiedzialna za wydawanie certyfikatów dla domen dla użytkowników. Usługa jest uruchamiania, jeśli lista szablonów certyfikatów zostaje załadowana poprzez kliknięcie przycisku **Odśwież listę** lub po wygenerowaniu certyfikatu.
7. W celu zapisania ustawień kliknij **OK**.

Po przeprowadzeniu integracji certyfikaty są generowane automatycznie.

Włączanie obsługi Kerberos Constrained Delegation

Aplikacja obsługuje użycie Kerberos Constrained Delegation.

W celu włączenia obsługi Kerberos Constrained Delegation:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.
2. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**.
3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.
4. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.
5. W oknie właściwości serwera iOS MDM wybierz sekcję **Ustawienia**.

6. W sekcji **Ustawienia** zaznacz pole **Zapewnij kompatybilność z Kerberos constrained delegation**.

7. Kliknij **OK**.

Dodawanie urządzeń mobilnych iOS do listy zarządzanych urządzeń

Aby dodać urządzenie mobilne iOS do listy zarządzanych urządzeń, współdzielony certyfikat musi zostać pobrany i zainstalowany na tym urządzeniu. Certyfikaty współdzielone są używane przez Serwer administracyjny do identyfikowania urządzeń mobilnych. Współdzielony certyfikat dla urządzenia mobilnego iOS jest dostarczany w obrębie profilu iOS MDM. Po dostarczeniu i zainstalowaniu współdzielonego certyfikatu na urządzeniu mobilnym, urządzenie pojawi się na liście zarządzanych urządzeń.

Kaspersky nie wspiera już Kaspersky Safe Browser.

Możesz dodać urządzenia mobilne użytkowników do listy zarządzanych urządzeń przy użyciu kreatora podłączania urządzenia mobilnego.

W celu połączenia urządzenia iOS z Serwerem administracyjnym przy użyciu certyfikatu współdzielonego:

1. Uruchom kreator podłączania urządzenia mobilnego w jeden z następujących sposobów:

   - Użyj menu kontekstowego z folderu **Konta użytkowników**:

     1. W drzewie konsoli rozwiń folder **Zaawansowane** i wybierz podfolder **Konta użytkowników**.

     2. W obszarze roboczym folderu **Konta użytkowników** wybierz użytkowników, grupy użytkowników lub grupy użytkowników Active Directory, dla których chcesz dodać urządzenia mobilne do listy zarządzanych urządzeń.

     3. Kliknij prawym klawiszem myszy i z menu kontekstowego konta użytkownika wybierz **Dodaj urządzenie mobilne**.

        Zostanie uruchomiony kreator podłączania urządzenia mobilnego.

   - W obszarze roboczym folderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

     1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Urządzenia mobilne**.

     2. W obszarze roboczym podfolderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

        Zostanie uruchomiony kreator podłączania urządzenia mobilnego.

2. W oknie **System operacyjny** kreatora, jako typ systemu operacyjnego wskaż **iOS**.

3. Na stronie **Wybieranie Serwera iOS MDM** wybierz serwer iOS MDM.

4. W oknie **Wybierz użytkowników, których urządzeniami mobilnymi chcesz zarządzać** wybierz użytkowników, grupy użytkowników lub grupy użytkowników Active Directory, których urządzenia mobilne chcesz dodać do listy zarządzanych urządzeń.

Ten krok jest pomijany, jeśli uruchamiasz kreator, wybierając element **Dodaj urządzenie mobilne** w menu kontekstowym folderu **Konta użytkowników**.

Jeśli chcesz dodać nowe konto użytkownika do listy, kliknij przycisk **Dodaj** i wprowadź właściwości konta użytkownika w otwartym oknie. Jeśli chcesz zmodyfikować lub przejrzeć właściwości konta użytkownika, wybierz konto użytkownika z listy i kliknij przycisk **Właściwości**.

5. W oknie **Źródło certyfikatu** określ metodę tworzenia współdzielonego certyfikatu, którego Serwer administracyjny użyje do identyfikacji urządzenia mobilnego. Certyfikat współdzielony można określić na jeden z następujących sposobów:

   - **Wystaw certyfikat przy użyciu narzędzi Serwera administracyjnego**

     Wybierz tę opcję, aby utworzyć nowy certyfikat przy użyciu narzędzi Serwera administracyjnego, jeśli wcześniej go nie utworzyłeś.

     Jeśli ta opcja jest zaznaczona, profil iOS MDM zostanie automatycznie podpisany przez certyfikat wygenerowany przez Serwer administracyjny.

     Opcja ta jest wybrana domyślnie.

   - **Określ plik certyfikatu**

     Wybierz tę opcję, aby określić plik certyfikatu, który został utworzony wcześniej.

     Ta metoda nie jest dostępna, jeśli w poprzednim kroku zaznaczono wielu użytkowników.

6. W oknie **Metoda powiadamiania użytkownika** zdefiniuj ustawienia powiadamiania użytkownika urządzenia mobilnego o utworzeniu certyfikatu za pośrednictwem wiadomości SMS lub wiadomości e-mail:

   - **Pokaż odnośnik w kreatorze**

     Jeśli wybierzesz tę opcję, łącze do pakietu instalacyjnego zostanie wyświetlone w ostatnim kroku kreatora połączeń urządzenia mobilnego.

     Ta opcja nie jest dostępna, jeśli dla połączenia urządzenia wybrano wielu użytkowników.

   - **Wyślij odnośnik do użytkownika**

     Zaznaczając tę opcję, zezwalasz na skonfigurowanie powiadamiania użytkownika o podłączeniu nowego urządzenia mobilnego.

     Możesz wybrać typ adresu e-mail, określić dodatkowy adres e-mail oraz zmodyfikować treść wiadomości. Możesz również wybrać typ telefonu użytkownika dla wysyłania wiadomości SMS, określić dodatkowy numer telefonu oraz zmodyfikować treść wiadomości SMS.

     Jeśli Serwer SMTP nie został skonfigurowany, wiadomości e-mail nie będą mogły być wysyłane do użytkowników Jeśli powiadomienia SMS nie zostały skonfigurowane, wiadomości SMS nie będą mogły być wysyłane do użytkowników.

7. W oknie **Wynik** kliknij przycisk **Zakończ**, aby zakończyć działanie kreatora.

Profil iOS MDM jest automatycznie publikowany na Kaspersky Security Center Web Server. Użytkownik urządzenia mobilnego odbiera powiadomienie z odnośnikiem do pobrania profilu iOS MDM z Serwera sieciowego. Użytkownik klika odnośnik. System operacyjny urządzenia mobilnego wyświetli pytanie o zaakceptowanie instalacji profilu iOS MDM. Użytkownik musi wyrazić zgodę na zainstalowanie profilu iOS MDM przed pobraniem profilu iOS MDM na urządzenie mobilne. Po pobraniu profilu iOS MDM i zsynchronizowaniu urządzenia mobilnego z Serwerem administracyjnym, urządzenie zostanie wyświetlone w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli.

Aby użytkownik mógł przejść na Kaspersky Security Center Web Server, korzystając z odnośnika, na urządzeniu mobilnym powinno być możliwe nawiązanie połączenia z Serwerem administracyjnym poprzez port 8061.

Dodawanie urządzeń mobilnych Android do listy zarządzanych urządzeń

Aby dodać urządzenie mobilne Android do listy zarządzanych urządzeń, Kaspersky Endpoint Security for Android i współdzielony certyfikat muszą zostać dostarczone i zainstalowane na urządzeniu mobilnym. Certyfikaty współdzielone są używane przez Serwer administracyjny do identyfikowania urządzeń mobilnych. Po dostarczeniu i zainstalowaniu współdzielonego certyfikatu na urządzeniu mobilnym, urządzenie pojawi się na liście zarządzanych urządzeń.

Możesz dodać urządzenia mobilne użytkowników do listy zarządzanych urządzeń przy użyciu kreatora podłączania urządzenia mobilnego. Kreator udostępnia dwie opcje dostarczenia i instalacji współdzielonego certyfikatu oraz Kaspersky Endpoint Security for Android:

- Przy użyciu odnośnika do Google Play
- Przy użyciu odnośnika z serwera sieci Web Kaspersky Security Center Web Server

  Pakiet instalacyjny Kaspersky Endpoint Security for Android przechowywany do dystrybucji na Serwerze administracyjnym jest używany do instalacji

Uruchamianie kreatora podłączania urządzenia mobilnego

W celu uruchomienia kreatora podłączania urządzenia mobilnego wykonaj jedną z następujących czynności:

- Użyj menu kontekstowego z folderu **Konta użytkowników**:

  1. W drzewie konsoli rozwiń folder **Zaawansowane** i wybierz podfolder **Konta użytkowników**.
  2. W obszarze roboczym folderu **Konta użytkowników** wybierz użytkowników, grupy użytkowników lub grupy użytkowników Active Directory, dla których chcesz dodać urządzenia mobilne do listy zarządzanych urządzeń.
  3. Kliknij prawym klawiszem myszy i z menu kontekstowego konta użytkownika wybierz **Dodaj urządzenie mobilne**.

     Zostanie uruchomiony kreator podłączania urządzenia mobilnego.

- W obszarze roboczym folderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

  1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Urządzenia mobilne**.

2. W obszarze roboczym podfolderu **Urządzenia mobilne** kliknij przycisk **Dodaj urządzenie mobilne**.

   Zostanie uruchomiony kreator podłączania urządzenia mobilnego.

Dodawanie urządzenia mobilnego Android przy użyciu odnośnika do Google Play

W celu zainstalowania Kaspersky Endpoint Security for Android i certyfikatu współdzielonego na urządzeniu mobilnym przy użyciu odnośnika do Google Play:

1. Uruchamianie kreatora podłączania urządzenia mobilnego.

2. W oknie **System operacyjny** kreatora, jako typ systemu operacyjnego urządzenia mobilnego wybierz **Android**.

3. W kroku **Metoda instalacji Kaspersky Endpoint Security for Android** wybierz **Przy użyciu odnośnika do Google Play**.

4. W oknie **Wybierz użytkowników, których urządzeniami mobilnymi chcesz zarządzać** wybierz użytkowników, grupy użytkowników lub grupy użytkowników Active Directory, dla których chcesz dodać urządzenia mobilne do listy zarządzanych urządzeń.

   Ten krok jest pomijany, jeśli uruchamiasz kreator, wybierając element **Dodaj urządzenie mobilne** w menu kontekstowym folderu **Konta użytkowników**.

   Jeśli chcesz dodać nowe konto użytkownika do listy, kliknij przycisk **Dodaj** i wprowadź właściwości konta użytkownika w otwartym oknie. Jeśli chcesz zmodyfikować lub przejrzeć właściwości konta użytkownika, wybierz konto użytkownika z listy i kliknij przycisk **Właściwości**.

5. W oknie **Źródło certyfikatu** określ metodę tworzenia współdzielonego certyfikatu, którego Serwer administracyjny użyje do identyfikacji urządzenia mobilnego. Certyfikat współdzielony można określić na jeden z następujących sposobów:

   - **Wystaw certyfikat przy użyciu narzędzi Serwera administracyjnego**

     Wybierz tę opcję, aby utworzyć nowy certyfikat przy użyciu narzędzi Serwera administracyjnego, jeśli wcześniej go nie utworzyłeś.

     Jeśli wybierzesz tę opcję, certyfikat zostanie automatycznie utworzony przy użyciu narzędzi Serwera administracyjnego.

     Opcja ta jest wybrana domyślnie.

   - **Określ plik certyfikatu**

     Wybierz tę opcję, aby określić plik certyfikatu, który został utworzony wcześniej.

     Ta metoda nie jest dostępna, jeśli w poprzednim kroku zaznaczono wielu użytkowników.

6. W oknie **Metoda powiadamiania użytkownika** zdefiniuj ustawienia powiadamiania użytkownika urządzenia mobilnego o utworzeniu certyfikatu za pośrednictwem wiadomości SMS lub wiadomości e-mail:

   - **Pokaż odnośnik w kreatorze**

Jeśli wybierzesz tę opcję, łącze do pakietu instalacyjnego zostanie wyświetlone w ostatnim kroku kreatora połączeń urządzenia mobilnego.

Ta opcja nie jest dostępna, jeśli dla połączenia urządzenia wybrano wielu użytkowników.

- **Wyślij odnośnik do użytkownika**

  Zaznaczając tę opcję, zezwalasz na skonfigurowanie powiadamiania użytkownika o podłączeniu nowego urządzenia mobilnego.

  Możesz wybrać typ adresu e-mail, określić dodatkowy adres e-mail oraz zmodyfikować treść wiadomości. Możesz również wybrać typ telefonu użytkownika dla wysyłania wiadomości SMS, określić dodatkowy numer telefonu oraz zmodyfikować treść wiadomości SMS.

  Jeśli Serwer SMTP nie został skonfigurowany, wiadomości e-mail nie będą mogły być wysyłane do użytkowników Jeśli powiadomienia SMS nie zostały skonfigurowane, wiadomości SMS nie będą mogły być wysyłane do użytkowników.

7. W oknie **Wynik** kliknij przycisk **Zakończ**, aby zakończyć działanie kreatora.

Po zakończeniu działania kreatora, odnośnik oraz kod QR zostaną wysłane na urządzenie mobilne użytkownika, umożliwiając mu w ten sposób pobranie Kaspersky Endpoint Security for Android. Użytkownik klika odnośnik lub skanuje kod QR. System operacyjny urządzenia mobilnego wyświetli pytanie o zaakceptowanie instalacji Kaspersky Endpoint Security for Android. Po pobraniu i zainstalowaniu Kaspersky Endpoint Security for Android, urządzenie mobilne nawiązuje połączenie z Serwerem administracyjnym i pobiera współdzielony certyfikat. Po zainstalowaniu certyfikatu na urządzeniu mobilnym, urządzenie zostanie wyświetlone w folderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli.

Dodawanie urządzenia mobilnego Android przy użyciu odnośnika z serwera sieci Web Kaspersky Security Center Web Server

Pakiet instalacyjny Kaspersky Endpoint Security for Android opublikowany na Serwerze administracyjnym zostanie użyty do instalacji.

W celu zainstalowania Kaspersky Endpoint Security for Android i certyfikatu współdzielonego na urządzeniu mobilnym przy użyciu odnośnika z serwera sieciowego:

1. Uruchamianie kreatora podłączania urządzenia mobilnego.
2. W oknie **System operacyjny** kreatora, jako typ systemu operacyjnego urządzenia mobilnego wybierz **Android**.
3. W kroku **Metoda instalacji Kaspersky Endpoint Security for Android** wybierz **Przy użyciu odnośnika z serwera sieci Web**.

   W polu, które się pojawi, wybierz pakiet instalacyjny lub utwórz nowy, klikając **Nowy**.
4. W oknie **Wybierz użytkowników, których urządzeniami mobilnymi chcesz zarządzać** wybierz użytkowników, grupy użytkowników lub grupy użytkowników Active Directory, dla których chcesz dodać urządzenia mobilne do listy zarządzanych urządzeń.

Ten krok jest pomijany, jeśli uruchamiasz kreator, wybierając element **Dodaj urządzenie mobilne** w menu kontekstowym folderu **Konta użytkowników**.

Jeśli chcesz dodać nowe konto użytkownika do listy, kliknij przycisk **Dodaj** i wprowadź właściwości konta użytkownika w otwartym oknie. Jeśli chcesz zmodyfikować lub przejrzeć właściwości konta użytkownika, wybierz konto użytkownika z listy i kliknij przycisk **Właściwości**.

5. W oknie **Źródło certyfikatu** określ metodę tworzenia współdzielonego certyfikatu, którego Serwer administracyjny użyje do identyfikacji urządzenia mobilnego. Certyfikat współdzielony można określić na jeden z następujących sposobów:

   - **Wystaw certyfikat przy użyciu narzędzi Serwera administracyjnego**

     Wybierz tę opcję, aby utworzyć nowy certyfikat przy użyciu narzędzi Serwera administracyjnego, jeśli wcześniej go nie utworzyłeś.

     Jeśli wybierzesz tę opcję, certyfikat zostanie automatycznie utworzony przy użyciu narzędzi Serwera administracyjnego.

     Opcja ta jest wybrana domyślnie.

   - **Określ plik certyfikatu**

     Wybierz tę opcję, aby określić plik certyfikatu, który został utworzony wcześniej.

     Ta metoda nie jest dostępna, jeśli w poprzednim kroku zaznaczono wielu użytkowników.

6. W oknie **Metoda powiadamiania użytkownika** zdefiniuj ustawienia powiadamiania użytkownika urządzenia mobilnego o utworzeniu certyfikatu za pośrednictwem wiadomości SMS lub wiadomości e-mail:

   - **Pokaż odnośnik w kreatorze**

     Jeśli wybierzesz tę opcję, łącze do pakietu instalacyjnego zostanie wyświetlone w ostatnim kroku kreatora połączeń urządzenia mobilnego.

     Ta opcja nie jest dostępna, jeśli dla połączenia urządzenia wybrano wielu użytkowników.

   - **Wyślij odnośnik do użytkownika**

     Zaznaczając tę opcję, zezwalasz na skonfigurowanie powiadamiania użytkownika o podłączeniu nowego urządzenia mobilnego.

     Możesz wybrać typ adresu e-mail, określić dodatkowy adres e-mail oraz zmodyfikować treść wiadomości. Możesz również wybrać typ telefonu użytkownika dla wysyłania wiadomości SMS, określić dodatkowy numer telefonu oraz zmodyfikować treść wiadomości SMS.

     Jeśli Serwer SMTP nie został skonfigurowany, wiadomości e-mail nie będą mogły być wysyłane do użytkowników Jeśli powiadomienia SMS nie zostały skonfigurowane, wiadomości SMS nie będą mogły być wysyłane do użytkowników.

7. W oknie **Wynik** kliknij przycisk **Zakończ**, aby zakończyć działanie kreatora.

Pakiet aplikacji mobilnej Kaspersky Endpoint Security for Android jest automatycznie publikowany na Kaspersky Security Center Web Server. Pakiet aplikacji mobilnej zawiera aplikację, ustawienia do łączenia urządzenia mobilnego z Serwerem administracyjnym, a także certyfikat. Użytkownik urządzenia mobilnego otrzymuje powiadomienie z odnośnikiem do pobrania pakietu z Serwera sieciowego. Użytkownik klika odnośnik. System operacyjny urządzenia wyświetla pytanie o zaakceptowanie instalacji pakietu aplikacji mobilnych. Jeśli użytkownik wyrazi zgodę, pakiet zostanie pobrany na urządzenie mobilne. Po pobraniu pakietu i zsynchronizowaniu urządzenia mobilnego z Serwerem administracyjnym, urządzenie zostanie wyświetlone w podfolderze **Urządzenia mobilne**, znajdującym się w folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli.

Zarządzanie urządzeniami mobilnymi Exchange ActiveSync

Ta sekcja opisuje zaawansowane funkcje zarządzania urządzeniami EAS poprzez Kaspersky Security Center.

Oprócz zarządzania urządzeniami EAS przy użyciu poleceń, administrator może używać następujących opcji:

- Utwórz profile zarządzania dla urządzeń EAS i przypisz je do skrzynek pocztowych użytkowników. *Profil zarządzania urządzeniem EAS* to profil Exchange ActiveSync, który jest używany na serwerze Microsoft Exchange do zarządzania urządzeniami EAS. W profilu zarządzania urządzeniem EAS możesz skonfigurować następujące grupy ustawień:
  - Ustawienia zarządzania hasłem użytkownika
  - Ustawienia synchronizacji poczty
  - Ograniczenia korzystania z funkcji urządzenia mobilnego
  - Ograniczenia korzystania z aplikacji mobilnych na urządzeniu mobilnym

  W zależności od modelu urządzenia mobilnego, ustawienia profilu zarządzającego mogą być stosowane częściowo. Stan zastosowanego profilu Exchange ActiveSync można zobaczyć we właściwościach urządzenia mobilnego.
- Wyświetl informacje dotyczące ustawień zarządzania urządzeniem EAS. Na przykład, we właściwościach urządzenia mobilnego administrator może sprawdzić godzinę ostatniej synchronizacji z serwerem Microsoft Exchange, numer ID urządzenia EAS, nazwę profilu Exchange ActiveSync oraz jego bieżący stan na urządzeniu mobilnym.
- Odłącz urządzenia EAS od funkcji zarządzania, jeśli nie są używane.
- Zdefiniuj ustawienia przeszukiwania Active Directory przez serwer urządzeń mobilnych Exchange, co umożliwia aktualizację informacji o urządzeniach mobilnych i skrzynkach pocztowych użytkowników.

Dodawanie profilu zarządzającego

Aby zarządzać urządzeniami EAS, możesz utworzyć profile zarządzania urządzeniami EAS oraz przypisać je do wybranych skrzynek pocztowych Microsoft Exchange.

Do skrzynki pocztowej Microsoft Exchange można przypisać tylko profil zarządzający urządzeniem EAS.

W celu dodania profilu zarządzającego urządzeniem EAS dla skrzynki pocztowej Microsoft Exchange:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.
2. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**.
3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer urządzeń mobilnych Exchange.
4. Z menu kontekstowego serwera urządzeń mobilnych Exchange wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera urządzeń mobilnych.
5. W oknie właściwości **Serwer urządzeń mobilnych Exchange** wybierz sekcję **Skrzynki pocztowe**.
6. Wybierz skrzynkę pocztową i kliknij przycisk **Przypisz profil**.

   Zostanie otwarte okno **Profile zasad**.
7. W oknie **Profile zasad** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Nowy profil**.
8. Skonfiguruj profil na zakładkach okna **Nowy profil**.
   - Jeśli chcesz określić nazwę profilu i przedział czasu aktualizacji, wybierz zakładkę **Ogólny**.
   - Jeśli chcesz skonfigurować hasło użytkownika urządzenia mobilnego, wybierz zakładkę **Hasło**.
   - Jeśli chcesz skonfigurować synchronizację z serwerem Microsoft Exchange, wybierz zakładkę **Synchronizacja**.
   - Jeśli chcesz skonfigurować ograniczenia funkcji urządzenia mobilnego, wybierz zakładkę **Ograniczenie dla funkcji**.
   - Jeśli chcesz skonfigurować ograniczenie użycia aplikacji mobilnych na urządzeniu mobilnym, wybierz zakładkę **Ograniczenia aplikacji**.
9. Kliknij **OK**.

   Nowy profil zostanie wyświetlony na liście profili, w oknie **Profile zasad**.

   Jeśli chcesz, żeby ten profil był automatycznie przypisywany do nowych skrzynek pocztowych, a także do tych, których profile zostały usunięte, wybierz go na liście profili i kliknij przycisk **Ustaw jako profil domyślny**.

   > Domyślny profil nie może zostać usunięty. Aby usunąć bieżący domyślny profil, musisz przypisać atrybut "profil domyślny" do innego profilu.
10. W oknie **Profile zasad** kliknij **OK**.

    Ustawienia profilu zarządzającego zostaną zastosowane na urządzeniu EAS przy następnej synchronizacji urządzenia z serwerem urządzeń mobilnych Exchange.

Usuwanie profilu zarządzającego

W celu usunięcia profilu zarządzającego urządzeniem EAS dla skrzynki pocztowej Microsoft Exchange:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.
2. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**.
3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer urządzeń mobilnych Exchange.
4. Z menu kontekstowego serwera urządzeń mobilnych Exchange wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera urządzeń mobilnych.
5. W oknie właściwości serwera urządzeń mobilnych Exchange wybierz sekcję **Skrzynki pocztowe**.
6. Wybierz skrzynkę pocztową i kliknij przycisk **Zmień profile**.

   Zostanie otwarte okno **Profile zasad**.
7. W oknie **Profile zasad** wybierz profil, który chcesz usunąć, i kliknij przycisk Usuń.

   Wybrany profil zostanie usunięty z listy profili zarządzających. Do urządzeń EAS zarządzanych przez usunięty profil zostanie zastosowany bieżący profil domyślny.

   > Jeśli chcesz usunąć bieżący profil domyślny, przydziel wartość „profil domyślny" do innego profilu, a następnie usuń wspomniany profil.

Zarządzanie profilami Exchange ActiveSync

Po zainstalowaniu serwera urządzeń mobilnych Exchange, w sekcji **Skrzynki pocztowe** okna właściwości Serwera możesz wyświetlić informacje dotyczące kont serwera Microsoft Exchange Server, które zostały pobrane poprzez przeszukiwanie aktualnej domeny lub lasu domeny.

Dodatkowo, w oknie właściwości serwera urządzeń mobilnych Exchange możesz użyć następujących przycisków:

- **Zmień profile** umożliwia otwarcie okna **Profile zasad**, które zawiera listę profili pobranych z serwera Microsoft Exchange Server. W tym oknie możesz utworzyć, zmodyfikować lub usunąć profile Exchange ActiveSync. Okno **Profile zasad** jest prawie takie samo jak okno do modyfikowania profilu w Konsoli zarządzania programu Exchange.
- **Przypisz profile do urządzeń mobilnych** — umożliwia przypisanie wybranego profilu Exchange ActiveSync do jednego lub kilku kont.
- **Włącz/wyłącz ActiveSync** — umożliwia włączenie lub wyłączenie Exchange ActiveSync HTTP dla jednego lub kilku kont.

Konfigurowanie obszaru skanowania

We właściwościach nowo zainstalowanego serwera urządzeń mobilnych Exchange, w sekcji **Ustawienia** możesz skonfigurować obszar skanowania. Domyślnie obszar skanowania to bieżąca domena, w której zainstalowany jest serwer urządzeń mobilnych Exchange. Wybranie wartości **Cały las domeny** rozszerzy obszar skanowania o cały las domen.

Praca z urządzeniami EAS

Urządzenia wykryte poprzez skanowanie serwera Microsoft Exchange Server zostaną dodane do standardowej listy urządzeń, która znajduje się w węźle **Zarządzanie urządzeniami mobilnymi**, w folderze **Urządzenia mobilne**.

Jeśli chcesz, żeby w folderze **Urządzenia mobilne** były wyświetlane tylko urządzenia Exchange ActiveSync (zwane również urządzeniami EAS), filtruj listę urządzeń, klikając odnośnik **Exchange ActiveSync (EAS)**, który znajduje się nad tą listą.

Urządzeniami EAS można zarządzać przy użyciu poleceń. Na przykład, polecenie **Przywróć ustawienia fabryczne** umożliwia usunięcie wszystkich danych z urządzenia i przywrócenie ustawień fabrycznych urządzenia. Polecenie jest przydatne, gdy urządzenie zostanie zgubione lub skradzione i będziesz chciał zapobiec uzyskaniu danych firmowych i osobowych przez pracowników firm trzecich.

Jeśli wszystkie dane zostały usunięte z urządzenia, zostaną ponownie usunięte przy kolejnym połączeniu urządzenia z serwerem Microsoft Exchange Server. Wykonanie polecenia będzie powtarzane, aż do usunięcia urządzenia z listy urządzeń. To zachowanie jest spowodowane przez zasady działania serwera Microsoft Exchange Server.

Aby usunąć urządzenie EAS z listy, w menu kontekstowym urządzenia wybierz **Usuń**. Jeśli konto Exchange ActiveSync nie zostało usunięte z urządzenia EAS, urządzenie to pojawi się ponownie na liście urządzeń po kolejnej synchronizacji urządzenia z serwerem Microsoft Exchange Server.

Przeglądanie informacji o urządzeniu EAS

W celu przejrzenia informacji o urządzeniu EAS:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia EAS, klikając odnośnik **Exchange ActiveSync (EAS)**.

3. Z menu kontekstowego urządzenia przenośnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości urządzenia EAS.

Okno właściwości urządzenia mobilnego wyświetla informacje o podłączonym urządzeniu EAS.

Odłączanie urządzenia EAS od funkcji zarządzania

W celu odłączenia urządzenia EAS od funkcji zarządzania przez serwer urządzeń mobilnych Exchange:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia EAS, klikając odnośnik **Exchange ActiveSync (EAS)**.

3. Wybierz urządzenie mobilne, które chcesz odłączyć od funkcji zarządzania przez serwer urządzeń mobilnych Exchange.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Usuń**.

Urządzenie EAS zostanie oznaczone jako przeznaczone do usunięcia przy użyciu ikony z czerwonym krzyżykiem. Urządzenie mobilne zostanie usunięte z listy zarządzanych urządzeń po jego usunięciu z bazy danych serwera Exchange ActiveSync. W tym celu administrator musi usunąć konto użytkownika z serwera Microsoft Exchange.

Uprawnienia użytkownika do zarządzania urządzeniami mobilnymi Exchange ActiveSync

W celu zarządzania urządzeniami mobilnymi działającymi na protokole Exchange ActiveSync z poziomu Microsoft Exchange Server 2010 lub Microsoft Exchange Server 2013, upewnij się, że użytkownik jest uwzględniony w grupie ról, dla której można wykonywać następujące polecenia commandlet:

- Get-CASMailbox
- Set-CASMailbox
- Remove-ActiveSyncDevice
- Clear-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Get-AcceptedDomain
- Set-AdServerSettings
- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy
- Remove-ActiveSyncMailboxPolicy

W celu zarządzania urządzeniami mobilnymi działającymi na protokole Exchange ActiveSync z poziomu Microsoft Exchange Server 2007, upewnij się, że użytkownik posiada uprawnienia administratora. Jeśli użytkownik nie posiada uprawnień, wykonaj polecenia commandlet w celu nadania użytkownikowi uprawnień administratora (patrz poniższa tabela).

Uprawnienia administratora wymagane do zarządzania urządzeniami mobilnymi Exchange ActiveSync dla Microsoft Exchange Server 2007

Dostęp	Obiekt	Cmdlet
Pełna	Gałąź "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	`Add-ADPermission -User <Na użytkownika> -Identity "CN Policies,CN=<Nazwa organizacji>,CN=Microsoft Exchange,CN=Services,CN=Co <Nazwa domeny>" -Inheritan AccessRight GenericAll`
Odczyt	Gałąź "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC= yourdomain"	`Add-ADPermission -User <Na użytkownika> -Identity "CN organizacji>,CN=Microsoft Exchange,CN=Services,CN=Co`

		`<Nazwa domeny>" -Inherita AccessRight GenericRead`
Odczyt/zapis	Właściwości msExchMobileMailboxPolicyLink i msExchOmaAdminWirelessEnable dla obiektów w Active Directory	`Add-ADPermission -User <Na użytkownika> -Identity "DC domeny>" -InheritanceType AccessRight ReadProperty,W Properties msExchMobileMai msExchOmaAdminWirelessEnab`
Pełna	Repozytoria skrzynki pocztowej dla ms-Exch-Store-Admin	`Get-MailboxDatabase | Add- User <nazwa użytkownika lu ExtendedRights ms-Exch-Sto`

Szczegółowe informacje dotyczące użycia poleceń commandlet w konsoli Exchange Management Shell można znaleźć na stronie działu pomocy technicznej Microsoft Exchange Server.

Zarządzanie urządzeniami iOS MDM

Ta sekcja opisuje zaawansowane funkcje zarządzania urządzeniami iOS MDM poprzez Kaspersky Security Center. Aplikacja obsługuje następujące funkcje zarządzania urządzeniami iOS MDM:

- Definiowanie ustawień zarządzanych urządzeń iOS MDM w trybie scentralizowanym i ograniczenie funkcji urządzeń przy użyciu profili konfiguracyjnych. Możesz dodać lub zmodyfikować profile konfiguracyjne, a także zainstalować je na urządzeniach mobilnych.
- Instalowanie aplikacji na urządzeniach mobilnych przy użyciu profili informacyjnych, omijając App Store. Na przykład możesz użyć profili informacyjnych do zainstalowania aplikacji firmowych na urządzeniach mobilnych użytkowników. Profil informacyjny zawiera informacje o aplikacji i urządzeniu mobilnym.
- Instalowanie aplikacji na urządzeniu iOS MDM poprzez App Store. Przed zainstalowaniem aplikacji na urządzeniu iOS MDM powinieneś dodać tę aplikację do serwera iOS MDM.

Co 24 godziny na wszystkie podłączone urządzenia mobilne iOS MDM wysyłane jest powiadomienie push w celu zsynchronizowania danych z serwerem iOS MDM.

Informacje o profilu konfiguracyjnym i profilu informacyjnym oraz aplikacjach zainstalowanych na urządzeniu z iOS MDM znajdziesz w oknie właściwości urządzenia.

Podpisywanie profilu iOS MDM za pomocą certyfikatu

Profil iOS MDM można podpisać za pomocą certyfikatu. Możesz użyć certyfikatu, który sam wystawiłeś, lub możesz otrzymać certyfikat od zaufanych urzędów certyfikacji.

W celu podpisania certyfikatu dla profilu iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.
2. Z otwartego menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.
3. W oknie właściwości folderu wybierz sekcję **Ustawienia połączenia dla urządzeń iOS**.
4. Kliknij przycisk **Przeglądaj** znajdujący się pod polem **Wybierz plik certyfikatu**.

Okno **Certyfikat**.

5. W polu **Typ certyfikatu** określ typ certyfikatu - publiczny lub prywatny:

   - Jeśli wybrana jest wartość **Kontener PKCS #12**, określ plik certyfikatu i hasło.
   - Jeśli wybrana jest wartość **Certyfikat X.509**:

     a. Określ plik klucza prywatnego (z rozszerzeniem *.prk lub *.pem).

     b. Określ hasło dla klucza prywatnego.

     c. Określ plik klucza publicznego (z rozszerzeniem *.cer).

6. Kliknij **OK**.

Profil iOS MDM jest podpisany za pomocą certyfikatu.

Dodawanie profilu konfiguracyjnego

Aby utworzyć profil konfiguracyjny, możesz użyć programu Apple Configurator 2, który jest dostępny na stronie Apple Inc. Apple Configurator 2 działa tylko na urządzeniach z systemem macOS; jeśli nie masz do dyspozycji takich urządzeń, możesz zamiast tego użyć narzędzia iPhone Configuration Utility na urządzeniu z zainstalowaną Konsolą administracyjną. Jednak firma Apple Inc. nie obsługuje już programu iPhone Configuration Utility.

W celu utworzenia profilu konfiguracyjnego przy użyciu iPhone Configuration Utility i dodania go do serwera iOS MDM:

1. W drzewie konsoli wybierz folder **Zarządzanie urządzeniami mobilnymi**.
2. W obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** wybierz podfolder **Serwery urządzeń mobilnych**.
3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.
4. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera urządzeń mobilnych.
5. W oknie właściwości serwera iOS MDM wybierz sekcję **Profile konfiguracyjne**.
6. W sekcji **Profile konfiguracyjne** kliknij przycisk **Utwórz**.

   Zostanie otwarte okno **Nowy profil konfiguracyjny**.
7. W oknie **Nowy profil konfiguracyjny** określ nazwę i numer ID profilu.

   Numer ID profilu konfiguracyjnego powinien być unikatowy; wartość powinna być określona w formacie Reverse-DNS (odwrotna translacja adresów DNS), na przykład: *com.companyname.identifier*.
8. Kliknij **OK**.

   Następnie zostanie uruchomione narzędzie iPhone Configuration Utility (jeśli jest zainstalowane).

9. Skonfiguruj ponownie profil konfiguracyjny w iPhone Configuration Utility.

   Opis ustawień profilu oraz instrukcje dotyczące sposobu konfiguracji profilu można znaleźć w dokumentacji załączonej do narzędzia iPhone Configuration Utility.

Po skonfigurowaniu profilu przy pomocy narzędzia iPhone Configuration Utility, nowy profil konfiguracyjny zostanie wyświetlony w sekcji **Profile konfiguracyjne**, w oknie właściwości serwera iOS MDM.

Kliknij przycisk **Modyfikuj**, aby zmodyfikować profil konfiguracyjny.

Kliknij przycisk **Importuj**, aby wczytać profil konfiguracyjny do programu.

Kliknij przycisk **Eksportuj**, aby zapisać profil konfiguracyjny do pliku.

Utworzony profil musi zostać zainstalowany na urządzeniach iOS MDM.

Instalowanie profilu konfiguracyjnego na urządzeniu

W celu zainstalowania profilu konfiguracyjnego na urządzeniu mobilnym:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM według typu protokołu (*iOS MDM*).

3. Wybierz urządzenie mobilne użytkownika, na którym chcesz zainstalować profil konfiguracyjny.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego zainstalowania profilu.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Zainstaluj profil** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z jego menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Zainstaluj profil**.

   Zostanie otwarte okno **Wybierz profile** wyświetlające listę profili. Wybierz z listy profil, który chcesz zainstalować na urządzeniu mobilnym. Możesz wybrać kilka profili do jednoczesnego zainstalowania na urządzeniu mobilnym. Aby wybrać kilka profili, użyj klawisza **Shift**. Aby wybrać grupę profili, użyj klawisza **CTRL**.

6. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrany profil konfiguracyjny zostanie zainstalowany na urządzeniu mobilnym użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia w raporcie poleceń zostanie wyświetlony jako *Gotowe*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

   Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

7. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Zainstalowany profil możesz sprawdzić i usunąć, jeśli jest to konieczne.

Usuwanie profilu konfiguracyjnego z urządzenia

W celu usunięcia profilu konfiguracyjnego z urządzenia mobilnego:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM, klikając odnośnik **iOS MDM**.

3. Wybierz urządzenie mobilne użytkownika, z którego chcesz usunąć profil konfiguracyjny.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego usunięcia profilu.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Usuń profil** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Usuń profil**.

   Zostanie otwarte okno **Usuń profile** wyświetlające listę profili.

6. Wybierz z listy profil, który chcesz usunąć z urządzenia mobilnego. Możesz wybrać kilka profili do jednoczesnego usunięcia z urządzenia mobilnego. Aby wybrać kilka profili, użyj klawisza **Shift**. Aby wybrać grupę profili, użyj klawisza **CTRL**.

7. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrany profil konfiguracyjny zostanie usunięty z urządzenia mobilnego użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia zostanie wyświetlony jako *Zakończone*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

   Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

8. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Dodanie nowego urządzenia poprzez opublikowanie odnośnika do profilu

W Konsoli administracyjnej administrator tworzy nowy profil iOS MDM za pomocą Kreatora instalacji certyfikatów. Kreator wykonuje następujące działania:

- Profil iOS MDM jest automatycznie publikowany na serwerze sieciowym.
- Do użytkownika zostaje wysłany odnośnik do profilu iOS MDM w wiadomości SMS lub e-mail. Po odebraniu wiadomości z odsyłaczem, użytkownik instaluje profil iOS MDM na urządzeniu mobilnym.
- Urządzenie mobilne łączy się z serwerem iOS MDM.

Ze względu na zaostrzoną politykę bezpieczeństwa, wprowadzoną przez firmę Apple, należy skonfigurować wersje protokołów TLS 1.1 i TLS 1.2 podczas łączenia urządzenia mobilnego działającego pod kontrolą systemu iOS 11 z Serwerem administracyjnym, na którym włączono integrację z Infrastrukturą klucza publicznego (PKI).

Dodanie nowego urządzenia mobilnego poprzez zainstalowanie profilu przez administratora

W celu połączenia urządzenia mobilnego z serwerem iOS MDM poprzez zainstalowanie profilu iOS MDM na tym urządzeniu mobilnym, administrator musi wykonać następujące czynności:

1. W Konsoli administracyjnej otwórz Kreator instalacji certyfikatu.
2. Utwórz nowy profil iOS MDM, zaznaczając pole wyboru **Pokaż certyfikat po zakończeniu działania kreatora**.
3. Zapisać profil iOS MDM.
4. Zainstalować profil iOS MDM na urządzeniu mobilnym użytkownika przy pomocy narzędzia Apple Configurator.

   Urządzenie mobilne łączy się z serwerem iOS MDM.

Ze względu na zaostrzoną politykę bezpieczeństwa, wprowadzoną przez firmę Apple, należy skonfigurować wersje protokołów TLS 1.1 i TLS 1.2 podczas łączenia urządzenia mobilnego działającego pod kontrolą systemu iOS 11 z Serwerem administracyjnym, na którym włączono integrację z Infrastrukturą klucza publicznego (PKI).

Dodawanie profilu informacyjnego

W celu dodania profilu informacyjnego do serwera iOS MDM:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.
2. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**.
3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.
4. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera urządzeń mobilnych.
5. W oknie właściwości **serwera iOS MDM** przejdź do sekcji **Profile informacyjne**.
6. W sekcji **Profile informacyjne** kliknij przycisk **Importuj** i określ ścieżkę dostępu do pliku profilu informacyjnego.

   Profil zostanie dodany do ustawień serwera iOS MDM.

   Kliknij przycisk **Eksportuj**, aby zapisać listę profili informacyjnych do pliku.

Możesz zainstalować profil informacyjny, który zaimportowałeś na urządzenia iOS MDM.

Instalowanie profilu informacyjnego na urządzeniu

W celu zainstalowania profilu informacyjnego na urządzeniu mobilnym:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM według typu protokołu (*iOS MDM*).

3. Wybierz urządzenie mobilne użytkownika, na którym chcesz zainstalować profil informacyjny.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego zainstalowania profilu informacyjnego.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Instalowanie profilu informacyjnego** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z jego menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Zainstaluj profil informacyjny**.

   Zostanie otwarte okno **Wybierz profile informacyjne** wyświetlające listę profili informacyjnych. Wybierz z listy profil informacyjny, który chcesz zainstalować na urządzeniu mobilnym. Możesz wybrać kilka profili informacyjnych do jednoczesnego zainstalowania ich na urządzeniu mobilnym. Aby wybrać kilka profili informacyjnych, użyj klawisza **Shift**. Aby wybrać grupę profili informacyjnych, użyj klawisza **Ctrl**.

6. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrany profil informacyjnych zostanie zainstalowany na urządzeniu mobilnym użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia w raporcie poleceń jest wyświetlony jako *Zakończone*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

   Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

7. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Zainstalowany profil możesz sprawdzić i usunąć, jeśli jest to konieczne.

Usuwanie profilu informacyjnego z urządzenia

W celu usunięcia profilu informacyjnego z urządzenia mobilnego:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM według typu protokołu (*iOS MDM*).

3. Wybierz urządzenie mobilne użytkownika, z którego chcesz usunąć profil informacyjny.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego usunięcia profilu informacyjnego.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Usuń profil informacyjny** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Usuń profil informacyjny**.

   Zostanie otwarte okno **Usuń profile informacyjne** wyświetlające listę profili.

6. Wybierz z listy profil informacyjny, który chcesz usunąć z urządzenia mobilnego. Możesz wybrać kilka profili informacyjnych do jednoczesnego usunięcia z urządzenia mobilnego. Aby wybrać kilka profili informacyjnych, użyj klawisza **Shift**. Aby wybrać grupę profili informacyjnych, użyj klawisza **Ctrl**.

7. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrany profil informacyjny zostanie usunięty z urządzenia mobilnego użytkownika. Aplikacje skojarzone z usuniętym profilem informacyjnym nie będą działać. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia zostanie wyświetlony jako *Zakończone*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

   Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

8. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Dodawanie zarządzanej aplikacji

Przed zainstalowaniem aplikacji na urządzeniu iOS MDM powinieneś dodać tę aplikację do serwera iOS MDM. Aplikacja jest postrzegana jako zarządzana, jeśli została zainstalowana na urządzeniu poprzez Kaspersky Security Center. Zarządzana aplikacja może być zarządzana ręcznie poprzez Kaspersky Security Center.

W celu dodania zarządzanej aplikacji do serwera iOS MDM:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.

2. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Serwery urządzeń mobilnych**.

3. W obszarze roboczym folderu **Serwery urządzeń mobilnych** wybierz serwer iOS MDM.

4. Z menu kontekstowego serwera iOS MDM wybierz **Właściwości**.

   Zostanie otwarte okno właściwości serwera iOS MDM.

5. W oknie właściwości serwera iOS MDM wybierz sekcję **Zarządzane aplikacje**.

6. W sekcji **Zarządzane aplikacje** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Dodaj aplikację**.

7. W oknie **Dodaj aplikację**, w polu **Nazwa aplikacji** określ nazwę dodawanej aplikacji.

8. W polu **Apple ID lub odnośnik do pliku manifestu** określ Apple ID dodawanej aplikacji lub określ odnośnik do pliku manifestu, który może być używany do pobrania aplikacji.

9. Jeśli chcesz, aby zarządzana aplikacja została usunięta z urządzenia mobilnego użytkownika wraz z profilem iOS MDM, zaznacz pole **Usuń wraz z profilem iOS MDM**.

10. Jeśli chcesz zablokować tworzenie kopii zapasowej danych aplikacji poprzez iTunes, zaznacz pole **Zablokuj kopię zapasową danych**.

11. Kliknij **OK**.

Dodana aplikacja będzie wyświetlana w sekcji **Zarządzane aplikacje** okna właściwości serwera iOS MDM.

Instalowanie aplikacji na urządzeniu mobilnym

W celu zainstalowania aplikacji na urządzeniu mobilnym iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. Wybierz urządzenie iOS MDM, na którym chcesz zainstalować aplikację.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego zainstalowania aplikacji.

3. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

4. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Zainstaluj aplikację** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z jego menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Zainstaluj aplikację**.

   Zostanie otwarte okno **Wybierz aplikacje** wyświetlające listę profili. Wybierz z listy aplikację, którą chcesz zainstalować na urządzeniu mobilnym. Możesz wybrać kilka aplikacji do jednoczesnego zainstalowania na urządzeniu mobilnym. Aby wybrać kilka aplikacji, użyj klawisza **Shift**. Aby wybrać grupę aplikacji, użyj klawisza **Ctrl**.

5. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrana aplikacja zostanie zainstalowana na urządzeniu mobilnym użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia w raporcie poleceń zostanie wyświetlony jako *Zakończone*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika. Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

6. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Informacje o zainstalowaniu aplikacji są wyświetlane we właściwościach urządzenia mobilnego iOS MDM. Możesz usunąć aplikację z urządzenia mobilnego, korzystając z raportu poleceń lub menu kontekstowego urządzenia mobilnego.

Usuwanie aplikacji z urządzenia

W celu usunięcia aplikacji z urządzenia mobilnego:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM według typu protokołu (*iOS MDM*).

3. Wybierz urządzenie mobilne użytkownika, z którego chcesz usunąć aplikację.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego usunięcia aplikacji.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Usuń aplikację** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z jego menu kontekstowego elementu **Wszystkie polecenia**, a następnie wybranie opcji **Usuń aplikację**.

   Zostanie otwarte okno **Usuń aplikacje** wyświetlające listę aplikacji.

6. Wybierz z listy aplikację, którą chcesz usunąć z urządzenia mobilnego. Możesz wybrać kilka aplikacji do ich jednoczesnego usunięcia. Aby wybrać kilka aplikacji, użyj klawisza **Shift**. Aby wybrać grupę aplikacji, użyj klawisza **Ctrl**.

7. Kliknij **OK**, aby wysłać polecenie na urządzenie mobilne.

   Po wykonaniu polecenia, wybrana aplikacja zostanie usunięta z urządzenia mobilnego użytkownika. Jeśli polecenie zostanie pomyślnie wykonane, bieżący stan polecenia zostanie wyświetlony jako *Zakończone*.

   Kliknij przycisk **Wyślij ponownie**, aby ponownie wysłać polecenie na urządzenie mobilne użytkownika.

   Kliknij przycisk **Usuń z kolejki**, aby anulować wykonanie wysłanego polecenia, jeśli ostatnie polecenie nie zostało jeszcze wykonane.

   Sekcja **Raport poleceń** wyświetla polecenia, które zostały wysłane na urządzenie mobilne, z odpowiednimi stanami wykonania. Kliknij **Odśwież**, aby zaktualizować listę poleceń.

8. Kliknij **OK**, aby zamknąć okno **Polecenia administracyjne urządzenia mobilnego**.

Konfigurowanie roamingu na urządzeniu mobilnym iOS MDM

W celu skonfigurowania roamingu:

1. W drzewie konsoli otwórz folder **Zarządzanie urządzeniami mobilnymi**.

2. W folderze **Zarządzanie urządzeniami mobilnymi** wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

3. Wybierz urządzenie iOS MDM należące do użytkownika, dla którego chcesz skonfigurować roaming.

   Możesz wybrać kilka urządzeń mobilnych do jednoczesnego skonfigurowania na nich roamingu.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

5. W oknie **Polecenia administracyjne urządzenia mobilnego** przejdź do sekcji **Konfiguruj roaming** i kliknij przycisk **Wyślij polecenie**.

   Polecenie możesz wysłać na urządzenie mobilne także poprzez wybranie z menu kontekstowego elementu **Wszystkie polecenia → Konfiguruj roaming**.

6. W oknie **Ustawienia roamingu** określ odpowiednie ustawienia:

- **Włącz roaming głosowy**

  Jeśli ta opcja jest włączona, na urządzeniach mobilnych iOS MDM zostanie włączony roaming połączeń. Użytkownik urządzenia mobilnego iOS MDM może wykonywać i odbierać połączenia w strefie roamingu.

  Domyślnie opcja ta jest włączona.

- **Włącz roaming danych**

  Jeśli ta opcja jest włączona, na urządzeniach mobilnych iOS MDM zostanie włączony roaming danych. Użytkownik urządzenia mobilnego iOS MDM może przeglądać internet w strefie roamingu.

  Domyślnie opcja ta jest wyłączona.

Roaming zostanie skonfigurowany dla wybranych urządzeń.

Przeglądanie informacji o urządzeniu iOS MDM

W celu przejrzenia informacji o urządzeniu iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM, klikając odnośnik **iOS MDM**.

3. Wybierz urządzenie mobilne, dla którego chcesz wyświetlić informacje.

4. Z menu kontekstowego urządzenia przenośnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości urządzenia iOS MDM.

Okno właściwości urządzenia mobilnego wyświetla informacje o podłączonym urządzeniu iOS MDM.

Odłączanie urządzenia iOS MDM od funkcji zarządzania

W celu odłączenia urządzenia iOS MDM od serwera iOS MDM:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia iOS MDM, klikając odnośnik **iOS MDM**.

3. Wybierz urządzenie mobilne, które chcesz odłączyć.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Usuń**.

Urządzenie iOS MDM zostanie oznaczone na liście jako obiekt do usunięcia. Urządzenie mobilne zostanie automatycznie usunięte z listy zarządzanych urządzeń po jego wcześniejszym usunięciu z bazy danych serwera iOS MDM. Urządzenie mobilne zostanie usunięte z bazy danych serwera iOS MDM w ciągu jednej minuty.

Po odłączeniu urządzenia iOS MDM od funkcji zarządzania, wszystkie zainstalowane profile konfiguracyjne, profil iOS MDM oraz aplikacje, dla których włączono opcję **Usuń wraz z profilem iOS MDM**, zostaną usunięte z urządzenia mobilnego.

Wysyłanie poleceń na urządzenie

W celu wysłania polecenia na urządzenie iOS MDM:

1. W Konsoli administracyjnej otwórz węzeł **Zarządzanie urządzeniami mobilnymi**.
2. Wybierz folder **Urządzenia mobilne**.
3. W folderze **Urządzenia mobilne** wybierz urządzenie mobilne, na które mają zostać wysłane polecenia.
4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.
5. Z wyświetlonej listy wybrać polecenie, które ma zostać wysłane na urządzenie mobilne.

Sprawdzanie stanu wykonania wysłanych poleceń

W celu sprawdzenia stanu wykonania polecenia, które zostało wysłane na urządzenie mobilne:

1. W Konsoli administracyjnej otwórz węzeł **Zarządzanie urządzeniami mobilnymi**.
2. Wybierz folder **Urządzenia mobilne**.
3. W folderze **Urządzenia mobilne** wybierz urządzenie mobilne, na którym ma być sprawdzony stan wykonania wybranych poleceń.
4. Z menu kontekstowego urządzenia mobilnego wybierz **Pokaż raport poleceń**.

Zarządzanie urządzeniami KES

W Kaspersky Security Center możesz zarządzać urządzeniami mobilnymi KES na następujące sposoby:

- Zarządzać urządzeniami KES w sposób scentralizowany przy pomocy poleceń.
- Przeglądać informacje dotyczące ustawień zarządzania urządzeniami KES.
- Instalować aplikacje przy użyciu pakietów aplikacji mobilnych.
- Odłączać urządzenia KES od funkcji zarządzania.

Tworzenie pakietów aplikacji mobilnych dla urządzeń KES

Aby możliwe było utworzenie pakietu aplikacji mobilnej dla urządzeń KES, niezbędna jest licencja Kaspersky Endpoint Security for Android.

W celu utworzenia pakietu aplikacji mobilnych:

1. W folderze **Zdalna instalacja** drzewa konsoli wybierz podfolder **Pakiety instalacyjne**.

   Domyślnie folder **Zdalna instalacja** to podfolder folderu **Zaawansowane**.

2. Kliknij przycisk **Akcje dodatkowe** i z listy rozwijalnej wybierz **Zarządzaj pakietami aplikacji mobilnych**.

3. W oknie **Zarządzanie pakietami aplikacji mobilnych** kliknij przycisk **Nowy**.

4. Zostanie uruchomiony Kreator tworzenia nowego pakietu. Postępuj zgodnie z instrukcjami kreatora.

Nowo utworzony pakiet aplikacji mobilnych jest wyświetlany w oknie **Zarządzanie pakietami aplikacji mobilnych**.

Włączanie uwierzytelniania opartego na certyfikatach urządzeń KES

Aby włączyć uwierzytelnianie oparte na certyfikacie urządzenia KES:

1. Otwórz rejestr systemu urządzenia klienckiego, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

2. Przejdź do gałęzi:

   - W systemach 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

   - W systemach 64-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

3. Utwórz klucz o nazwie LP_MobileMustUseTwoWayAuthOnPort13292.

4. Jako typ klucza określ REG_DWORD.

5. Dla klucza wskaż wartość 1.

6. Uruchom ponownie usługę Serwera administracyjnego.

Obowiązkowe uwierzytelnianie oparte na certyfikacie urządzenia KES przy użyciu współdzielonego certyfikatu zostanie włączone po uruchomieniu usługi Serwera administracyjnego.

> Pierwsze nawiązanie połączenia między urządzeniem KES i Serwerem administracyjnym nie wymaga certyfikatu.

Domyślnie uwierzytelnianie oparte na certyfikatach urządzeń KES jest wyłączone.

Przeglądanie informacji o urządzeniu KES

W celu przejrzenia informacji o urządzeniu KES:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia KES według typu protokołu (*KES*).

3. Wybierz urządzenie mobilne, dla którego chcesz wyświetlić informacje.

4. Z menu kontekstowego urządzenia przenośnego wybierz **Właściwości**.

   Zostanie otwarte okno właściwości urządzenia KES.

Okno właściwości urządzenia mobilnego wyświetla informacje o podłączonym urządzeniu KES.

Odłączanie urządzenia KES od funkcji zarządzania

Aby odłączyć urządzenie KES od funkcji zarządzania, użytkownik musi usunąć Agenta sieciowego z urządzenia mobilnego. Po usunięciu Agenta sieciowego, szczegóły urządzenia mobilnego zostaną usunięte z bazy danych Serwera administracyjnego, a administrator będzie mógł usunąć urządzenie mobilne z listy zarządzanych urządzeń.

W celu usunięcia urządzenia KES z listy zarządzanych urządzeń:

1. W folderze **Zarządzanie urządzeniami mobilnymi** drzewa konsoli wybierz podfolder **Urządzenia mobilne**.

   Obszar roboczy folderu wyświetla listę zarządzanych urządzeń mobilnych.

2. W obszarze roboczym przefiltruj urządzenia KES według typu protokołu (*KES*).

3. Wybierz urządzenie mobilne, które chcesz odłączyć od funkcji zarządzania.

4. Z menu kontekstowego urządzenia mobilnego wybierz **Usuń**.

   Urządzenie mobilne zostanie usunięte z listy zarządzanych urządzeń.

   Jeśli program Kaspersky Endpoint Security for Android nie został usunięty z urządzenia mobilnego, po synchronizacji z Serwerem administracyjnym to urządzenie mobilne ponownie pojawi się na liście zarządzanych urządzeń.

Szyfrowanie i ochrona danych

Szyfrowanie danych zmniejsza ryzyko przypadkowego wycieku danych w sytuacji, gdy notebook, nośnik wymienny lub dysk twardy zostanie skradziony lub zgubiony, bądź też, gdy dostęp do danych uzyskują nieautoryzowani użytkownicy lub aplikacje.

Kaspersky Endpoint Security for Windows oferuje funkcję szyfrowania. Kaspersky Endpoint Security for Windows umożliwia szyfrowanie plików przechowywanych na dyskach lokalnych urządzeń i nośnikach wymiennych, a także całych nośników wymiennych i dysków twardych.

Reguły szyfrowania są konfigurowane przy użyciu Kaspersky Security Center, poprzez profile. Zgodnie z określonymi regułami, szyfrowanie i deszyfrowanie jest wykonywane po zastosowaniu profilu.

Dostępność funkcji zarządzania szyfrowaniem jest określana przez ustawienia interfejsu.

Administrator może wykonywać następujące akcje:

- Konfigurować i przeprowadzać szyfrowanie lub deszyfrowanie plików na dyskach lokalnych urządzenia.
- Konfigurować oraz przeprowadzać szyfrowanie plików na nośnikach wymiennych.
- Tworzyć reguły dostępu aplikacji do zaszyfrowanych plików.
- Tworzyć i przekazywać użytkownikowi plik klucza dostępu do zaszyfrowanych plików, jeśli funkcja szyfrowania pliku posiada ograniczenia na urządzeniu użytkownika.
- Konfigurować i wykonywać szyfrowanie dysku twardego.
- Zarządzać dostępem użytkownika do zaszyfrowanych dysków twardych i nośników wymiennych (zarządzać kontami Agenta autoryzacji, tworzyć i dostarczać użytkownikom informacje dotyczące przywrócenia nazwy konta i hasła, a także klucze dostępu do zaszyfrowanych urządzeń).
- Wyświetlać stany szyfrowania i raporty dotyczące szyfrowania plików.

Działania te są wykonywane przy użyciu narzędzi zintegrowanych z Kaspersky Endpoint Security for Windows. Szczegółowe instrukcje dotyczące wykonywania działań oraz opis funkcji szyfrowania są dostępne w internetowym systemie pomocy dla Kaspersky Endpoint Security for Windows.

Kaspersky Security Center obsługuje funkcjonalność zarządzania szyfrowaniem dla urządzeń z systemem operacyjnym macOS. Szyfrowanie jest konfigurowane przy użyciu narzędzi Kaspersky Endpoint Security for Mac dla tych wersji aplikacji, które obsługują funkcję szyfrowania. Szczegółowe instrukcje dotyczące wykonywania operacji oraz opis funkcji szyfrowania można znaleźć w Podręczniku administratora *Kaspersky Endpoint Security for Mac*.

Przeglądanie listy zaszyfrowanych urządzeń

W celu przejrzenia listy urządzeń, na których przechowywane są zaszyfrowane informacje:

1. Z drzewa konsoli Serwera administracyjnego wybierz folder **Szyfrowanie i ochrona danych**.
2. Otwórz listę zaszyfrowanych urządzeń przy użyciu jednej z następujących metod:
   - Klikając odnośnik **Przejdź do listy zaszyfrowanych dysków** w sekcji **Zarządzanie zaszyfrowanymi dyskami**.
   - Wybierając folder **Zaszyfrowane dyski** w drzewie konsoli.

W obszarze roboczym zostaną wyświetlone informacje o urządzeniach w sieci, na których przechowywane są zaszyfrowane pliki, oraz o urządzeniach zaszyfrowanych na poziomie dysku. Po odszyfrowaniu informacji na urządzeniu, urządzenie jest automatycznie usuwane z listy.

Informacje przedstawione na liście urządzeń mogą być sortowane (rosnąco lub malejąco) według dowolnej kolumny.

Ustawienia interfejsu użytkownika określają, czy folder **Szyfrowanie i ochrona danych** jest wyświetlany w drzewie konsoli.

Wyświetlanie listy zdarzeń szyfrowania

Podczas wykonywania zadań szyfrowania lub deszyfrowania danych na urządzeniach, Kaspersky Endpoint Security for Windows wysyła do Kaspersky Security Center informacje o zdarzeniach następujących typów:

- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak wolnego miejsca na dysku.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na problemy z licencją.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak uprawnień dostępu.
- Dla aplikacji zablokowano dostęp do zaszyfrowanego pliku.
- Nieznane błędy.

W celu wyświetlenia listy zdarzeń, które wystąpiły w trakcie szyfrowania danych na urządzeniach:

1. Z drzewa konsoli Serwera administracyjnego wybierz folder **Szyfrowanie i ochrona danych**.
2. Przejdź do listy zdarzeń występujących podczas szyfrowania, korzystając z jednej z następujących metod:
   - Klikając odnośnik **Przejdź do listy błędów** w sekcji **Błędy szyfrowania danych**.
   - Wybierając folder **Zaszyfrowane dyski** w drzewie konsoli.

W obszarze roboczym zostaną wyświetlone informacje o problemach, które wystąpiły podczas szyfrowania danych na urządzeniach.

Na liście zdarzeń szyfrowania można wykonywać następujące działania:

- Sortować dane w dowolnej kolumnie rosnąco lub malejąco.
- Wykonywać szybkie wyszukiwanie wpisów (przez dopasowanie tekstu podciągiem znaków w dowolnym polu listy).
- Eksportować listę zdarzeń do pliku tekstowego.

Ustawienia interfejsu użytkownika określają, czy folder **Szyfrowanie i ochrona danych** jest wyświetlany w drzewie konsoli.

Eksportowanie listy zdarzeń szyfrowania do pliku tekstowego

W celu wyeksportowania listy zdarzeń szyfrowania do pliku tekstowego:

1. Utwórz listę zdarzeń szyfrowania.

2. Z menu kontekstowego listy zdarzeń wybierz **Eksportuj listę**.

   Zostanie otwarte okno **Eksportuj listę**.

3. W oknie **Eksportuj listę** określ nazwę pliku tekstowego z listą zdarzeń, wybierz folder zapisu i kliknij przycisk **Zapisz**.

   Lista zdarzeń szyfrowania zostanie zapisana w określonym pliku.

Tworzenie i przeglądanie raportów z szyfrowania

Możesz wygenerować następujące raporty:

- Raport o stanie szyfrowania zarządzanych urządzeń. Ten raport zawiera szczegółowe informacje na temat szyfrowania danych na różnych zarządzanych urządzeniach. Na przykład raport pokazuje liczbę urządzeń, do których ma zastosowanie polityka ze skonfigurowanymi regułami szyfrowania. Możesz także dowiedzieć się, na przykład, ile urządzeń wymaga ponownego uruchomienia. Raport zawiera również informacje o technologii i algorytmie szyfrowania dla każdego urządzenia.

- Raport o stanie szyfrowania urządzeń pamięci masowej. Ten raport zawiera podobne informacje jak raport o stanie szyfrowania zarządzanych urządzeń, ale zawiera dane tylko dla urządzeń pamięci masowej i dysków wymiennych.

- Raport o prawach dostępu do zaszyfrowanych dysków. Ten raport pokazuje, które konta użytkowników mają dostęp do zaszyfrowanych dysków.

- Raport o błędach podczas szyfrowania plików. Ten raport zawiera informacje o błędach, które wystąpiły podczas uruchamiania zadań szyfrowania lub deszyfrowania danych na urządzeniach.

- Raport o zablokowanym dostępie do zaszyfrowanych plików. Ten raport zawiera informacje o blokowaniu dostępu aplikacji do zaszyfrowanych plików. Ten raport jest pomocny, jeśli nieautoryzowany użytkownik lub aplikacja próbuje uzyskać dostęp do zaszyfrowanych plików lub dysków.

W celu wygenerowania raportu dotyczącego szyfrowania urządzeń:

1. Z drzewa konsoli wybierz folder **Szyfrowanie i ochrona danych**.

2. Wykonaj jedną z poniższych czynności:

   - Aby wygenerować raport dotyczący stanu szyfrowania zarządzanych urządzeń, kliknij odnośnik **Wyświetl raport o szyfrowaniu urządzeń pamięci masowej**.

     Jeśli jeszcze nie skonfigurowano tego raportu, zostanie uruchomiony Kreator tworzenia nowego szablonu raportu. Postępuj zgodnie z krokami kreatora.

   - Aby wygenerować raport dotyczący stanu szyfrowania urządzeń pamięci masowej, w drzewie konsoli wybierz podfolder **Zaszyfrowane dyski**, a następnie kliknij przycisk **Wyświetl raport o szyfrowaniu urządzeń pamięci masowej**.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

W celu wygenerowania raportu o uprawnieniach dostępu do zaszyfrowanych urządzeń:

1. Z drzewa konsoli wybierz folder **Szyfrowanie i ochrona danych**.

2. Wykonaj jedną z poniższych czynności:

- Kliknij odnośnik **Raport o prawach dostępu do zaszyfrowanych dysków** w sekcji **Zarządzanie zaszyfrowanymi dyskami**, aby uruchomić Kreator tworzenia nowego szablonu raportu.

- Wybierz podfolder **Zaszyfrowane dyski**, a następnie kliknij przycisk **Raport o prawach dostępu do zaszyfrowanych dysków**, aby uruchomić Kreator tworzenia nowego szablonu raportu.

3. Postępuj zgodnie z instrukcjami kreatora tworzenia nowego szablonu raportu.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

W celu wygenerowania raportu o błędach szyfrowania plików:

1. Z drzewa konsoli wybierz folder **Szyfrowanie i ochrona danych**.

2. Wykonaj jedną z poniższych czynności:

   - Kliknij odnośnik **Wyświetl raport o błędach podczas szyfrowania plików,** dostępny w sekcji **Błędy szyfrowania danych**, aby uruchomić Kreator tworzenia nowego szablonu raportu.

   - Wybierz podfolder **Zdarzenia szyfrowania**, a następnie kliknij odnośnik **Raport o błędach szyfrowania plików**, aby uruchomić Kreator tworzenia nowego szablonu raportu.

3. Postępuj zgodnie z instrukcjami kreatora tworzenia nowego szablonu raportu.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

W celu wygenerowania raportu o stanie szyfrowania zarządzanych urządzeń:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.

3. Kliknij przycisk **Nowy szablon raportu**, aby uruchomić Kreator tworzenia nowego szablonu raportu.

4. Postępuj zgodnie z instrukcjami kreatora tworzenia nowego szablonu raportu. W oknie **Wybieranie typu szablonu raportu**, w sekcji **Inny** wybierz **Raport o stanie szyfrowania zarządzanych urządzeń**.

   Po zakończeniu pracy kreatora tworzenia nowego szablonu raportu, nowy szablon raportu pojawi się w węźle Serwer administracyjny, na zakładce **Raporty**.

5. W węźle odpowiedniego Serwera administracyjnego, na zakładce **Raporty** wybierz szablon raportu, który został utworzony w poprzednich krokach instrukcji.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

Możesz również zapoznać się z informacjami o spełnianiu warunków profilu szyfrowania przez stan szyfrowania urządzeń i nośników wymiennych, które są dostępne na panelach informacyjnych, na zakładce **Statystyki**, w węźle Serwer administracyjny.

W celu wygenerowania raportu o blokowaniu dostępu do zaszyfrowanych plików:

1. Z drzewa konsoli wybierz węzeł z nazwą żądanego Serwera administracyjnego.

2. W obszarze roboczym węzła wybierz zakładkę **Raporty**.

3. Kliknij przycisk **Nowy szablon raportu**, aby uruchomić Kreator tworzenia nowego szablonu raportu.

4. Postępuj zgodnie z instrukcjami kreatora tworzenia nowego szablonu raportu. W oknie **Wybieranie typu szablonu raportu**, w sekcji **Inny** wybierz **Raport o zablokowanym dostępie do zaszyfrowanych plików**.

   Po zakończeniu pracy kreatora tworzenia nowego szablonu raportu, nowy szablon raportu pojawi się w węźle **Serwer administracyjny**, na zakładce **Raporty**.

5. W węźle **Serwer administracyjny**, na zakładce **Raporty** wybierz szablon raportu, który został utworzony w poprzednich krokach instrukcji.

Zostanie rozpoczęte tworzenie raportu. Raport pojawi się na zakładce **Raporty** węzła **Serwer administracyjny**.

Przesyłanie kluczy szyfrowania między Serwerami administracyjnymi

Jeśli funkcja szyfrowania danych jest włączona na zarządzanym urządzeniu, klucz szyfrowania jest przechowywany na Serwerze administracyjnym. Klucz szyfrowania służy do uzyskiwania dostępu do zaszyfrowanych danych i zarządzania zasadą szyfrowania.

Klucz szyfrowania musi zostać przesłany do innego Serwera administracyjnego w następujących przypadkach:

- Ponownie skonfiguruj Agenta sieciowego na zarządzanym urządzeniu, aby przypisać urządzenie do innego Serwera administracyjnego. Jeśli to urządzenie zawiera zaszyfrowane dane, klucz szyfrowania musi zostać przesłany do docelowego Serwera administracyjnego. W przeciwnym razie dane nie mogą zostać odszyfrowane.

- Szyfrujesz dysk wymienny podłączony do urządzenia D1 zarządzanego przez Serwer administracyjny S1, a następnie podłączasz ten dysk wymienny do urządzenia D2 zarządzanego przez Serwer administracyjny S2. Aby uzyskać dostęp do danych na dysku wymiennym, klucz szyfrowania musi zostać przesłany z Serwera administracyjnego S1 do Serwera administracyjnego S2.

- Zaszyfrujesz plik na urządzeniu D1 zarządzanym przez Serwer administracyjny S1, a następnie próbujesz uzyskać dostęp do pliku na urządzeniu D2 zarządzanym przez Serwer administracyjny S2. Aby uzyskać dostęp do pliku, klucz szyfrowania musi zostać przesłany z Serwera administracyjnego S1 do Serwera administracyjnego S2.

Możesz przesłać klucze szyfrowania na następujące sposoby:

- Automatycznie, włączając opcję **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** we właściwościach dwóch Serwerów administracyjnych, między którymi należy przesłać klucz szyfrowania. Jeśli ta opcja jest wyłączona dla jednego z Serwerów administracyjnych, automatyczne przesyłanie kluczy szyfrowania nie jest możliwe.

  Jeśli włączysz opcję **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** we właściwościach Serwera administracyjnego, Serwer administracyjny wyśle wszystkie klucze szyfrowania przechowywane w swoim repozytorium do głównego Serwera administracyjnego (jeśli istnieje) o jeden poziom wyżej w hierarchii.

  Podczas próby uzyskania dostępu do zaszyfrowanych danych Serwer administracyjny najpierw wyszukuje klucz szyfrowania we własnym repozytorium. Jeśli opcja **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania** jest włączona, a żądany klucz szyfrowania nie został znaleziony w repozytorium, Serwer administracyjny dodatkowo wyśle żądanie do głównych Serwerów administracyjnych (jeśli istnieją) w celu dostarczenia żądanego klucza szyfrowania. Żądanie zostanie wysłane na wszystkie główne Serwery administracyjne, aż do serwera na najwyższym poziomie hierarchii.

- Ręcznie z jednego Serwera administracyjnego na inny, eksportując i importując plik zawierający klucze szyfrowania.

  Eksportowanie i importowanie kluczy szyfrowania to czynności uwzględnione w funkcji zarządzania kluczami szyfrowania. Aby wykonać te akcje, skonfiguruj prawa dostępu do funkcji dla użytkowników Kaspersky Security Center w następujący sposób:

- Przyznaj prawo dostępu **Odczyt** do funkcji zarządzania kluczami szyfrowania użytkownikowi, który eksportuje klucze szyfrowania z pomocniczego Serwera administracyjnego.

- Przyznaj prawo dostępu **Wpisz** do funkcji zarządzania kluczami szyfrowania użytkownikowi, który importuje klucze szyfrowania na docelowy Serwer administracyjny.

W celu włączenia automatycznego przesyłania kluczy szyfrowania między Serwerami administracyjnymi w obrębie hierarchii:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz włączyć automatyczne przesyłanie kluczy szyfrowania.

2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

3. W oknie właściwości wybierz sekcję **Algorytm szyfrowania**.

4. Włącz opcję **Użyj hierarchii Serwerów administracyjnych, aby uzyskać klucze szyfrowania**.

5. Kliknij **OK**, aby zastosować zmiany.

Klucze szyfrowania zostaną przesłane na główne Serwery administracyjne (jeśli istnieją) przy kolejnej synchronizacji (puls). Ten Serwer administracyjny dostarczy również, na żądanie, klucz szyfrowania ze swojego repozytorium do podrzędnego Serwera administracyjnego.

W celu ręcznego przesyłania kluczy szyfrowania między Serwerami administracyjnymi:

1. W drzewie konsoli Serwera administracyjnego wybierz podrzędny Serwer administracyjny, z którego chcesz przesyłać klucze szyfrowania.

2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

3. W oknie właściwości wybierz sekcję **Algorytm szyfrowania**.

4. Kliknij **Wyeksportuj klucze szyfrowania z Serwera administracyjnego**.

   Upewnij się, że użytkownik, który eksportuje klucze szyfrowania z serwera, ma przyznane prawo dostępu **Odczyt** do funkcji zarządzania kluczami szyfrowania.

5. W oknie **Eksportuj klucze szyfrowania**:

   - Kliknij przycisk **Przeglądaj**, a następnie określ, gdzie należy zapisać plik.

   - Określ hasło do ochrony pliku przed nieautoryzowanym dostępem.

     Zapamiętaj hasło. Utraconego hasła nie można odzyskać. Jeśli hasło zostanie utracone, należy powtórzyć procedurę eksportowania. Dlatego zanotuj hasło i miej je pod ręką.

6. Prześlij plik na inny Serwer administracyjny, na przykład, poprzez folder współdzielony lub nośnik wymienny.

7. Na docelowym Serwerze administracyjnym upewnij się, że Konsola administracyjna Kaspersky Security Center jest uruchomiona.

8. W drzewie konsoli Serwera administracyjnego wybierz docelowy Serwer administracyjny, gdzie chcesz przesłać klucze szyfrowania.

9. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
10. W oknie właściwości wybierz sekcję **Algorytm szyfrowania**.
11. Kliknij **Zaimportuj klucze szyfrowania do Serwera administracyjnego**.

    Upewnij się, że użytkownik, który eksportuje klucze szyfrowania z serwera, ma przyznane prawo dostępu **Wpisz** do funkcji zarządzania kluczami szyfrowania.
12. W oknie **Importuj klucze szyfrowania**:
    - Kliknij przycisk **Przeglądaj**, a następnie wybierz plik zawierający klucze szyfrowania.
    - Określ hasło.
13. Kliknij **OK**.

Klucze szyfrowania są przesyłane na docelowy Serwer administracyjny.

Repozytoria danych

Ta sekcja zawiera informacje o danych przechowywanych na Serwerze administracyjnym i używanych do śledzenia stanu urządzeń klienckich oraz sposobie zarządzania nimi.

Folder **Repozytoria** drzewa konsoli wyświetla dane używane do śledzenia stanów urządzeń klienckich.

Folder **Repozytoria** zawiera następujące obiekty:

- Uaktualnienia pobrane przez Serwer administracyjny, które mogą zostać rozesłane na urządzenia klienckie
- Listę sprzętu wykrytego w sieci
- Klucze licencyjne wykryte na urządzeniach klienckich
- Pliki umieszczone w folderach Kwarantanny na urządzeniach przez aplikacje zabezpieczające
- Pliki umieszczone w Kopii zapasowej na urządzeniach klienckich
- Pliki, dla których odroczono skanowanie przez aplikacje antywirusowe

Eksportowanie listy obiektów w repozytorium do pliku tekstowego

Możesz wyeksportować listę obiektów z repozytorium do pliku tekstowego.

W celu wyeksportowania listy obiektów z repozytorium do pliku tekstowego:

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder odpowiedniego repozytorium.
2. W podfolderze repozytorium, z menu kontekstowego wybierz **Eksportuj listę**.

   Zostanie otwarte okno **Eksportuj listę**, w którym możesz określić nazwę pliku tekstowego i ścieżkę do folderu, w którym się znajduje.

Pakiety instalacyjne

Kaspersky Security Center umieszcza pakiety instalacyjne aplikacji firmy Kaspersky oraz firm trzecich w repozytoriach danych.

Pakiet instalacyjny to zestaw plików niezbędnych do instalacji aplikacji. Pakiet instalacyjny zawiera ustawienia instalacyjne i wstępnej konfiguracji aplikacji.

Jeśli chcesz zainstalować aplikację na urządzeniu klienckim, utwórz dla niej pakiet instalacyjny lub użyj istniejącego pakietu. Lista utworzonych pakietów instalacyjnych znajduje się w drzewie konsoli, w folderze **Zdalna instalacja**, w podfolderze **Pakiety instalacyjne**.

Główne stany plików w repozytorium

Aplikacje zabezpieczające skanują pliki na urządzeniach w poszukiwaniu znanych wirusów i innych programów, które mogą stwarzać zagrożenie, przydzielają stany do plików i umieszczają niektóre z nich w repozytorium.

Aplikacje zabezpieczające mogą, na przykład:

- Zapisać kopię pliku w repozytorium przed jego usunięciem
- Odizolować prawdopodobnie zainfekowane pliki w repozytorium

Stany plików zostały przedstawione w poniższej tabeli. Możesz uzyskać więcej informacji o działaniach podejmowanych na plikach w odpowiednich systemach pomocy aplikacji zabezpieczających.

Stany plików w repozytorium

Nazwa stanu	Opis stanu
Zainfekowany	Plik zawiera sekcję kodu znanego wirusa lub innego szkodliwego programu, którego informacje zostały wykryte w antywirusowych bazach danych Kaspersky.
Niezainfekowany	W pliku nie wykryto znanych wirusów ani innych szkodliwych programów.
Ostrzeżenie	Plik zawiera fragment kodu, który częściowo odpowiada fragmentowi kodu znanego zagrożenia.
Prawdopodobnie zainfekowany	Plik zawiera zmodyfikowany kod znanego wirusa lub kod przypominający wirusa, który nie jest jeszcze znany Kaspersky.
Umieszczony w folderze przez użytkownika	Użytkownik ręcznie umieścił plik w repozytorium, ponieważ zachowanie pliku wzbudzało podejrzenie, że może on zawierać jakieś zagrożenia. Użytkownik może przeskanować plik w poszukiwaniu zagrożeń z użyciem aktualnych baz danych.
Fałszywy alarm	Aplikacja Kaspersky przydzieliła stan Zainfekowany do niezainfekowanego pliku, ponieważ jego kod jest podobny do kodu wirusa. Po przeskanowaniu pliku z użyciem aktualnych baz danych, plik zostaje zidentyfikowany jako niezainfekowany.
Wyleczony	Plik został pomyślnie wyleczony.
Usunięty	Plik został usunięty podczas przetwarzania.
Zabezpieczony hasłem	Plik nie może zostać przetworzony, ponieważ jest chroniony hasłem.

Wywoływanie reguł w trybie Inteligentne uczenie

Ta sekcja zawiera informacje o wykrywaniu obiektów, wykonywanym przez reguły Adaptacyjnej kontroli anomalii w Kaspersky Endpoint Security for Windows na urządzeniach klienckich.

Reguły wykrywają nietypowe zachowania na urządzeniach klienckich i mogą je zablokować. Jeśli reguły działają w trybie Inteligentne uczenie, wykrywają nietypowe zachowania i wysyłają raporty o każdym takim wystąpieniu do Serwera administracyjnego Kaspersky Security Center. Te informacje są przechowywane pod postacią listy w podfolderze **Wywoływanie reguł w trybie Inteligentne uczenie się** folderu **Repozytoria**. Możesz potwierdzić wykrycie obiektów jako poprawne lub dodać je jako wykluczenia, żeby ten typ zachowania nie był już uznawany za nietypowy.

Informacje o wykrytych obiektach są przechowywane w dzienniku zdarzeń na Serwerze administracyjnym (wraz z innymi zdarzeniami) i w raporcie Adaptacyjnej kontroli anomalii.

Więcej informacji o Adaptacyjnej kontroli anomalii, regułach, ich trybach i stanach można znaleźć w pomocy Kaspersky Endpoint Security for Windows.

Przeglądanie listy obiektów wykrytych przy użyciu reguł Adaptacyjnej kontroli anomalii

W celu przejrzenia listy obiektów wykrytych przez reguły Adaptacyjnej kontroli anomalii:

1. W drzewie konsoli wybierz węzeł Serwera administracyjnego, którego potrzebujesz.
2. Wybierz podfolder **Wywoływanie reguł w trybie Inteligentne uczenie się** (domyślnie jest to podfolder **Zaawansowane → Repozytoria**).

   Lista wyświetla następujące informacje o obiektach wykrytych przy użyciu reguł Adaptacyjnej kontroli anomalii:

   - **Grupa administracyjna**

     Nazwa grupy administracyjnej, do której należy urządzenie.

   - **Nazwa urządzenia**

     Nazwa urządzenia klienckiego, do którego reguła została zastosowana.

   - **Nazwa**

     Nazwa zastosowanej reguły.

   - **Stan**

Wykluczanie—jeśli administrator przetworzył ten element i dodał go jako wykluczenie do reguł. Ten stan pozostanie do kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym; po synchronizacji element zniknie z listy.

Potwierdzanie—jeśli administrator przetworzył ten element i zatwierdził go. Ten stan pozostanie do kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym; po synchronizacji element zniknie z listy.

Pusty—jeśli administrator nie przetworzył tego elementu.

- **Łączna liczba wyzwoleń reguł**

  Liczba wykryć w obrębie jednej reguły heurystycznej, jeden proces i jedno urządzenie klienckie. Ta liczba jest zliczana przez Kaspersky Endpoint Security.

- **Nazwa użytkownika**

  Nazwa użytkownika urządzenia klienckiego, który uruchomił proces, który wygenerował wykrycie.

- **Ścieżka procesu źródłowego**

  Ścieżka do procesu źródłowego, czyli do procesu, który wykonuje akcję (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna procesu źródłowego**

  Suma kontrolna SHA-256 pliku procesu źródłowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Ścieżka obiektu źródłowego**

  Ścieżka do obiektu, który uruchomił proces (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna obiektu źródłowego**

  Suma kontrolna SHA-256 pliku źródłowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Ścieżka procesu docelowego**

  Ścieżka do procesu docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna procesu docelowego**

  Suma kontrolna SHA-256 pliku docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Ścieżka obiektu docelowego**

  Ścieżka do obiektu docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Suma kontrolna obiektu docelowego**

  Suma kontrolna SHA-256 pliku docelowego (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security).

- **Przetworzono**

  Data wykrycia anomalii.

W celu wyświetlenia właściwości każdego elementu informacji:

1. W drzewie konsoli wybierz węzeł Serwera administracyjnego, którego potrzebujesz.
2. Wybierz podfolder **Wywoływanie reguł w trybie Inteligentne uczenie się** (domyślnie jest to podfolder **Zaawansowane → Repozytoria**).
3. W obszarze roboczym **Wywoływanie reguł w trybie Inteligentne uczenie się** wybierz żądany obiekt.
4. Wykonaj jedną z poniższych czynności:
   - Kliknij odnośnik **Właściwości** w oknie z informacjami, które pojawi się w prawej części okna.
   - W menu kontekstowym kliknij prawym klawiszem myszy i wybierz **Właściwości**.

   Zostanie otwarte okno właściwości obiektu, wyświetlające informacje o wybranym elemencie.

Możesz potwierdzić lub dodać do wykluczeń dowolny element z listy wykrytych obiektów reguł Adaptacyjnej kontroli anomalii.

W celu zatwierdzenia elementu:

Wybierz element (lub kilka elementów) na liście wykrytych obiektów i kliknij przycisk **Potwierdź**.

Stan elementu(ów) zostanie zmieniony na **Potwierdzanie**.

Twoje potwierdzenie zostanie uwzględnione w statystykach używanych przez reguły (więcej informacji znajdziesz w pomocy do Kaspersky Endpoint Security 11 for Windows).

W celu dodania elementu jako wykluczenia:

Kliknij prawym klawiszem element (lub kilka elementów) na liście wykrytych obiektów i w menu kontekstowym wybierz **Dodaj do wykluczeń**.

Zostanie uruchomiony Kreator dodawania wykluczenia. Postępuj zgodnie z instrukcjami kreatora.

Jeśli odrzucisz lub zatwierdzisz element, zostanie on wykluczony z listy wykrytych obiektów po kolejnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym i już nie pojawi się na liście.

Dodawanie wykluczeń z reguł Adaptacyjnej kontroli anomalii

Kreator dodawania wykluczenia umożliwia dodanie wykluczeń z reguł Adaptacyjnej kontroli anomalii dla Kaspersky Endpoint Security.

Możesz uruchomić kreator poprzez jedną z trzech poniższych procedur.

W celu uruchomienia kreatora dodawania wykluczenia poprzez węzeł Adaptacyjna kontrola anomalii:

1. Z drzewa konsoli wybierz węzeł żądanego Serwera administracyjnego.
2. Wybierz **Wywoływanie reguł w trybie Inteligentne uczenie się** (domyślnie jest to podfolder **Zaawansowane → Repozytoria**).
3. W obszarze roboczym kliknij prawym klawiszem element (lub kilka elementów) na liście wykrytych obiektów i wybierz **Dodaj do wykluczeń**.

   Za jednym razem możesz dodać do 1000 wykluczeń. Jeśli wybierzesz więcej elementów i spróbujesz dodać je do wykluczeń, zostanie wyświetlona wiadomość o błędzie.

Zostanie uruchomiony Kreator dodawania wykluczenia.

Możesz uruchomić Kreator dodawania wykluczenia z innych węzłów w drzewie konsoli:

- Zakładki **Zdarzenia** okna głównego Serwera administracyjnego (następnie opcja **Żądania użytkownika** lub opcja **Ostatnie zdarzenia**).
- **Raportu o stanie reguł Adaptacyjnej kontroli anomalii**, kolumny **Liczba wykryć**.

Krok 1. Wybieranie aplikacji

Ten krok może zostać pominięty, jeśli posiadasz tylko jedną wersję Kaspersky Endpoint Security for Windows i nie posiadasz innych aplikacji, które obsługują reguł Adaptacyjnej kontroli anomalii.

Kreator dodawania wykluczenia wyświetla listę aplikacji firmy Kaspersky, których wtyczki zarządzające umożliwiają dodawanie wykluczeń do profili dla tych aplikacji. Wybierz aplikację z listy i kliknij **Dalej**, aby przejść do wyboru profilu, do którego zostanie dodane wykluczenie.

Krok 2. Wybieranie zasady (zasad)

kreator wyświetla listę profili (z profilami zasad) dla Kaspersky Endpoint Security.

Wybierz wszystkie profile i zasady, do których chcesz dodać wykluczenia, a następnie kliknij **Dalej**.

Krok 3. Przetwarzanie zasady (zasad)

kreator wyświetla pasek postępu podczas przetwarzania profili. Możesz przerwać przetwarzanie profili, klikając **Anuluj**.

Profili dziedziczonych nie można aktualizować. Jeśli nie masz uprawnień do modyfikowania profilu, ten profil też nie zostanie zaktualizowany.

Jeśli wszystkie profile są przetwarzane (lub jeśli przerwiesz przetwarzanie), zostanie wyświetlony raport. Pokazuje, które profile zostały zaktualizowane pomyślnie (zielona ikona), a które profile nie zostały zaktualizowane (czerwona ikona).

Jest to ostatni krok kreatora. Kliknij **Zakończ**, aby zamknąć kreator.

Kwarantanna i Kopia zapasowa

Aplikacje antywirusowe firmy Kaspersky, zainstalowane na urządzeniach klienckich, podczas skanowania urządzenia mogą umieszczać pliki w Kwarantannie lub Kopii zapasowej.

Kwarantanna jest specjalnym repozytorium, w którym przechowywane są potencjalnie zainfekowane pliki oraz pliki, które nie mogły zostać wyleczone w momencie wykrycia.

Kopia zapasowa została zaprojektowana do przechowywania kopii zapasowych plików, które w wyniku procesu leczenia zostały usunięte lub zmodyfikowane.

Kaspersky Security Center tworzy listę plików umieszczonych w Kwarantannie lub Kopii zapasowej przez aplikacje Kaspersky zainstalowane na urządzeniach. Agenty sieciowe na urządzeniach klienckich przesyłają informacje o plikach w Kwarantannie i Kopii zapasowej do Serwera administracyjnego. Przy użyciu Konsoli administracyjnej możesz przeglądać właściwości plików przechowywanych w repozytoriach na urządzeniach, uruchamiać skanowanie w zakresie złośliwego oprogramowania tych repozytoriów i usuwać przechowywane pliki. Ikony stanów plików są opisane w dodatku.

Praca z folderami Kwarantanna i Kopia zapasowa jest możliwa w programach Kaspersky Anti-Virus for Windows Workstations i Kaspersky Anti-Virus for Windows Servers w wersjach 6.0 i nowszych, jak również w Kaspersky Endpoint Security 10 for Windows i nowszych wersjach.

Kaspersky Security Center nie kopiuje plików z repozytoriów do Serwera administracyjnego. Wszystkie pliki są przechowywane w repozytoriach na urządzeniach. Plik można przywrócić tylko na urządzeniu z zainstalowaną aplikacją antywirusową, która umieściła plik w repozytorium.

Włączanie zdalnego zarządzania dla plików w repozytoriach

Domyślnie, nie możesz zarządzać plikami umieszczonymi w repozytoriach na urządzeniach klienckich.

W celu włączenia zdalnego zarządzania plikami przechowywanymi w repozytoriach na urządzeniach klienckich:

1. Z drzewa konsoli wybierz grupę administracyjną, dla której chcesz włączyć zdalne zarządzanie dla plików w repozytorium.
2. W obszarze roboczym grupy otwórz zakładkę **Zasady**.
3. Na zakładce **Zasady** wybierz profil aplikacji zabezpieczającej, która umieściła pliki w repozytoriach na urządzeniach.
4. W oknie ustawień profilu, w grupie ustawień **Przesyłanie danych do Serwera administracyjnego** zaznacz pola odpowiadające repozytoriom, dla których chcesz włączyć zdalne zarządzanie.

Lokalizacja grupy ustawień **Przesyłanie danych do Serwera administracyjnego** w oknie właściwości profilu i nazwy pól zależą od aktualnie używanej aplikacji zabezpieczającej.

Przeglądanie właściwości pliku umieszczonego w repozytorium

W celu przejrzenia właściwości pliku w Kwarantannie lub Kopii zapasowej:

1. Z drzewa konsoli wybierz folder **Repozytoria**, a z niego podfolder **Kwarantanna** lub **Kopia zapasowa**.
2. W obszarze roboczym folderu **Kwarantanna** (**Kopia zapasowa**) wybierz plik, którego właściwości chcesz przejrzeć.
3. Z menu kontekstowego pliku wybierz polecenie **Właściwości**.

Usuwanie plików z repozytoriów

W celu usunięcia pliku z Kwarantanny lub Kopii zapasowej:

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Kwarantanna** lub **Kopia zapasowa**.
2. W obszarze roboczym folderu **Kwarantanna** (lub **Kopia zapasowa**) zaznacz pliki, które chcesz usunąć, przy użyciu klawisza **Shift** lub **Ctrl**.
3. Usuń pliki w jeden z następujących sposobów:
   - Wybierając **Usuń** z menu kontekstowego plików.
   - Klikając odnośnik **Usuń** (**Usuń**, jeżeli chcesz usunąć jeden plik) w oknie z informacjami dla wybranych plików.

Aplikacje zabezpieczające, które umieściły pliki w repozytoriach na urządzeniach klienckich, usuną te same pliki z tych repozytoriów.

Przywracanie plików z repozytoriów

W celu przywrócenia pliku z Kwarantanny lub Kopii zapasowej:

1. Z drzewa konsoli wybierz folder **Repozytoria**, a z niego podfolder **Kwarantanna** lub **Kopia zapasowa**.
2. W obszarze roboczym folderu **Kwarantanna** (**Kopia zapasowa**) zaznacz pliki, które chcesz przywrócić, przy użyciu klawisza **Shift** lub **Ctrl**.
3. Uruchom przywracanie plików w jeden z następujących sposobów:
   - Wybierając **Przywróć** z menu kontekstowego plików.
   - Klikając odnośnik **Przywróć** w oknie z informacjami dla wybranych plików.

Aplikacje zabezpieczające, które umieściły pliki w repozytoriach na urządzeniach klienckich, przywrócą te same pliki do ich oryginalnych folderów.

Zapisywanie plików z repozytoriów na dysku

Kaspersky Security Center umożliwia zapisanie na dysku kopii plików, które zostały umieszczone przez aplikację zabezpieczającą w Kwarantannie lub Kopii zapasowej na urządzeniu klienckim. Pliki są kopiowane do określonego folderu na urządzeniu, na którym jest zainstalowany program Kaspersky Security Center.

W celu zapisania kopii pliku z Kwarantanny lub Kopii zapasowej na dysku twardym:

1. Z drzewa konsoli wybierz folder **Repozytoria**, a z niego podfolder **Kwarantanna** lub **Kopia zapasowa**.
2. W obszarze roboczym folderu **Kwarantanna** (**Kopia zapasowa**) wybierz plik, który chcesz skopiować na dysk twardy.
3. Uruchom kopiowanie w jeden z następujących sposobów:
   - Wybierając z menu kontekstowego pliku element **Zapisz na dysku**.
   - Klikając odnośnik **Zapisz na dysku** dostępny w oknie z informacjami dla wybranego pliku.

Aplikacja zabezpieczająca, która umieściła plik w Kwarantannie na urządzeniu klienckim, zapisze kopię tego pliku w określonym folderze.

Skanowanie plików w Kwarantannie

W celu przeskanowania plików poddanych kwarantannie:

1. Z drzewa konsoli wybierz folder **Repozytoria**, a z niego podfolder **Kwarantanna**.
2. W obszarze roboczym folderu **Kwarantanna** zaznacz pliki, które chcesz przeskanować, przy użyciu klawisza **`Shift`** lub **`Ctrl`**.
3. Uruchom skanowanie pliku w jeden z następujących sposobów:
   - Wybierając **Skanuj** z menu kontekstowego pliku.
   - Klikając odnośnik **Skanuj** w oknie z informacjami dla wybranych plików.

   Aplikacja uruchomi zadanie skanowania na żądanie dla aplikacji zabezpieczających, które umieściły wybrane pliki w Kwarantannie na urządzeniach, na których te pliki są przechowywane.

Aktywne zagrożenia

Informacje o nieprzetworzonych plikach wykrytych na urządzeniach klienckich są przechowywane w folderze **Repozytoria**, w podfolderze **Aktywne zagrożenia**.

Odroczone przetwarzanie i leczenie plików jest wykonywane przez aplikację antywirusową na żądanie lub po wystąpieniu określonego zdarzenia. Możesz skonfigurować odroczone przetwarzanie.

Leczenie nieprzetworzonego pliku

W celu uruchomienia leczenia nieprzetworzonego pliku:

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Aktywne zagrożenia**.
2. W obszarze roboczym folderu **Aktywne zagrożenia** wybierz plik, który chcesz wyleczyć.
3. Uruchom leczenie pliku w jeden z następujących sposobów:
   - Wybierając **Wylecz** z menu kontekstowego pliku.
   - Klikając odnośnik **Wylecz** w oknie z informacjami dla wybranego pliku.

Podjęta zostanie próba wyleczenia tego pliku.

Jeśli plik zostanie wyleczony, aplikacja antywirusowa, zainstalowana na urządzeniu klienckim, przywróci go do oryginalnego folderu. Wpis dotyczący pliku zostanie usunięty z listy w folderze **Aktywne zagrożenia**. Jeśli pliku nie można wyleczyć, aplikacja antywirusowa, zainstalowana na urządzeniu, usunie go z tego urządzenia. Wpis dotyczący pliku zostanie usunięty z listy w folderze **Aktywne zagrożenia**.

Zapisywanie nieprzetworzonego pliku na dysku

Kaspersky Security Center umożliwia zapisywanie na dysku kopii nieprzetworzonych plików, wykrytych na urządzeniach klienckich. Pliki są kopiowane do określonego folderu na urządzeniu, na którym jest zainstalowany program Kaspersky Security Center. Możesz pobrać plik tylko wtedy, gdy jest on przechowywany w magazynie kopii zapasowej zarządzanego urządzenia.

W celu zapisania kopii nieprzetworzonego pliku na dysku:

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Aktywne zagrożenia**.
2. W obszarze roboczym folderu **Aktywne zagrożenia** wybierz pliki, które chcesz skopiować na dysk.
3. Uruchom kopiowanie w jeden z następujących sposobów:
   - Wybierając z menu kontekstowego pliku element **Zapisz na dysku**.
   - Klikając odnośnik **Zapisz na dysku** dostępny w oknie z informacjami dla wybranego pliku.

Aplikacja zabezpieczająca, zainstalowana na urządzeniu klienckim, na którym wykryto nieprzetworzony plik, zapisze kopię tego pliku w określonym folderze.

Usuwanie plików z folderu „Aktywne zagrożenia”

*W celu usunięcia pliku z folderu **Aktywne zagrożenia**:*

1. W drzewie konsoli, w folderze **Repozytoria** wybierz podfolder **Aktywne zagrożenia**.
2. W obszarze roboczym folderu **Aktywne zagrożenia** zaznacz pliki, które chcesz usunąć, przy użyciu klawiszy **Shift** i **Ctrl**.
3. Usuń pliki w jeden z następujących sposobów:
   - Wybierając **Usuń** z menu kontekstowego plików.

- Klikając odnośnik **Usuń** (**Usuń**, jeżeli chcesz usunąć jeden plik) w oknie z informacjami dla wybranych plików.

Aplikacje zabezpieczające, które umieściły pliki w repozytoriach na urządzeniach klienckich, usuną te same pliki z tych repozytoriów. Wpisy dotyczące plików zostaną usunięte z listy w folderze **Aktywne zagrożenia**.

Kaspersky Security Network (KSN)

Ta sekcja opisuje sposób korzystania z infrastruktury usług online o nazwie Kaspersky Security Network (KSN). Sekcja zawiera szczegóły dotyczące KSN, a także instrukcje związane z włączaniem KSN, konfiguracją dostępu do KSN oraz wyświetlaniem statystyk korzystania z serwera proxy KSN.

Informacje o KSN

Kaspersky Security Network (KSN) jest to usługa sieciowa oferująca dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky po wykryciu zagrożeń, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. KSN umożliwia korzystanie z baz danych reputacji firmy Kaspersky, z których pobierane są informacje o aplikacjach zainstalowanych na zarządzanych urządzeniach.

Kaspersky Security Center obsługuje następujące rozwiązania infrastrukturalne KSN:

- *Globalna sieć KSN* to rozwiązanie umożliwiające wymianę informacji z Kaspersky Security Network. Uczestnicząc w KSN, wyrażasz zgodę na wysyłanie do Kaspersky w trybie automatycznym informacji dotyczących działania aplikacji firmy Kaspersky, zainstalowanych na urządzeniach klienckich, które są zarządzane przez Kaspersky Security Center. Informacje są wysyłane zgodnie z bieżącymi ustawieniami dostępu KSN. Analitycy firmy Kaspersky dodatkowo analizują otrzymane informacje i umieszczają je w reputacyjnych i statystycznych bazach danych Kaspersky Security Network. Kaspersky Security Center domyślnie korzysta z tego rozwiązania.

- *Private KSN* to rozwiązanie, które umożliwia użytkownikom urządzeń z zainstalowanymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów. Kaspersky Private Security Network (Private KSN) jest przeznaczony dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z jednego z następujących powodów:

  - Urządzenia użytkowników nie są podłączone do internetu.

  - Przekazywanie jakichkolwiek danych poza granice kraju lub poza korporacyjną sieć LAN jest zabronione przez prawo lub ograniczone przez korporacyjną politykę bezpieczeństwa.

  Możesz skonfigurować ustawienia dostępu do Kaspersky Private Security Network w sekcji **Ustawienia KSN Proxy** w oknie właściwości Serwera administracyjnego.

Aplikacja wyświetla pytanie o przyłączenie się do KSN podczas działania kreatora wstępnej konfiguracji. Można rozpocząć lub zakończyć korzystanie z KSN w dowolnym momencie, podczas korzystania z aplikacji.

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji lub uaktualniania Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz nadal korzystać z KSN zgodnie z poprzednią wersją Oświadczenia KSN, które zaakceptowałeś wcześniej.

Gdy KSN jest włączone, Kaspersky Security Center sprawdza, czy serwery KSN są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić utrzymanie poziomu bezpieczeństwa zarządzanych urządzeń.

Urządzenia klienckie zarządzane przez Serwer administracyjny wchodzą w interakcję z KSN poprzez serwer proxy KSN. Serwer proxy KSN posiada następujące cechy:

- Urządzenia klienckie mogą wysyłać żądania do KSN oraz przesyłać informacje do KSN nawet wtedy, gdy nie mają bezpośredniego dostępu do internetu.
- Serwer KSN proxy buforuje przetwarzane dane, ograniczając obciążenie połączenia wychodzącego i czas oczekiwania na informacje żądane przez urządzenie klienckie.

Możesz skonfigurować serwer proxy KSN w sekcji **Ustawienia KSN Proxy** w oknie właściwości Serwera administracyjnego.

Konfigurowanie dostępu do Kaspersky Security Network

Możesz skonfigurować dostęp do Kaspersky Security Network (KSN) na Serwerze administracyjnym i na punkcie dystrybucji.

W celu skonfigurowania dostępu Serwera administracyjnego do Kaspersky Security Network (KSN):

1. W drzewie konsoli należy wybrać Serwer administracyjny, dla którego chcesz skonfigurować dostęp do KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w panelu **Sekcje** wybierz **KSN Proxy** → **Ustawienia KSN Proxy**.
4. W obszarze roboczym włącz opcję **Użyj Serwera administracyjnego** jako serwera proxy, aby włączyć usługę KSN Proxy.

   Dane są wysyłane z urządzeń klienckich do KSN zgodnie z profilem Kaspersky Endpoint Security, który jest aktywny na tych urządzeniach klienckich. Jeśli to pole jest odznaczone, żadne dane nie będą wysyłane do KSN z Serwera administracyjnego i urządzeń klienckich poprzez Kaspersky Security Center. Jednakże urządzenia klienckie mogą wysyłać dane bezpośrednio do KSN (z pominięciem Kaspersky Security Center) zgodnie z ich ustawieniami. Profil Kaspersky Endpoint Security for Windows, aktywny na urządzeniach klienckich, określa, które dane będą wysyłane bezpośrednio z tych urządzeń do KSN (z pominięciem Kaspersky Security Center).
5. Włącz opcję **Zgadzam się na korzystanie z Kaspersky Security Network**.

   Jeśli ta opcja jest włączona, urządzenia klienckie będą wysyłać wyniki instalacji łat do Kaspersky. Przed włączeniem tej opcji należy przeczytać i zaakceptować warunki Oświadczenia KSN.

   Jeśli używasz Prywatnej sieci KSN, włącz opcję **Konfiguruj Private KSN** i kliknij przycisk **Wybierz plik z ustawieniami KSN Proxy**, aby pobrać ustawienia prywatnej sieci KSN (pliki z rozszerzeniami pkcs7 i pem). Po pobraniu ustawień, interfejs wyświetla kontakty i nazwę dostawcy, a także datę utworzenia pliku z ustawieniami prywatnej sieci KSN.

   Jeśli włączyłeś prywatną sieć KSN, zwróć uwagę na punkty dystrybucji skonfigurowane do wysyłania żądań KSN bezpośrednio do Cloud KSN. Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej) będzie nadal wysyłał żądania KSN do Cloud KSN. Aby ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do prywatnej sieci KSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji. Możesz włączyć tę opcję we właściwościach punktu dystrybucji lub w zasadzie Agenta sieciowego.

Jeśli zaznaczysz pole **Konfiguruj Private KSN**, pojawi się wiadomość ze szczegółami dotyczącymi prywatnej sieci KSN.

Prywatna sieć KSN jest obsługiwana przez następujące aplikacje firmy Kaspersky:

- Kaspersky Security Center
- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

Jeśli włączysz opcję **Konfiguruj Private KSN** w Kaspersky Security Center, te aplikacje otrzymają informację o obsłudze prywatnej sieci KSN. W oknie ustawień aplikacji, w podsekcji **Kaspersky Security Network** sekcji **Zaawansowana ochrona przed zagrożeniami** wyświetlana jest informacja **Dostawca KSN: prywatna sieć KSN**. W innym przypadku, wyświetlana będzie informacja **Dostawca KSN: globalna sieć KSN**.

Jeśli podczas działania prywatnej sieci KSN korzystasz z wcześniejszej wersji aplikacji Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 lub Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent, zalecamy korzystanie z podrzędnych Serwerów administracyjnych, dla których włączono korzystanie z prywatnej sieci KSN.

Kaspersky Security Center nie wysyła żadnych danych statystycznych do Kaspersky Security Network, jeśli prywatna sieć KSN została skonfigurowana w sekcji **KSN Proxy** → **Ustawienia KSN Proxy** okna właściwości Serwera administracyjnego.

Jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach Serwera administracyjnego, ale Twoja sieć wymaga, abyś korzystał bezpośrednio z prywatnej sieci KSN, włącz opcję **Ignoruj ustawienia serwera proxy w przypadku łączenia z Private KSN**. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do Private KSN.

6. Skonfiguruj połączenie Serwera administracyjnego z usługą KSN proxy:
   - W sekcji **Ustawienia połączenia**, w polu **Port TCP** określ numer portu TCP, który będzie używany do nawiązywania połączenia z serwerem proxy KSN. Domyślny port do nawiązywania połączenia z serwerem KSN proxy to 13111.
   - Jeśli chcesz, żeby Serwer administracyjny nawiązywał połączenie z serwerem proxy KSN poprzez port UDP, włącz opcję **Użyj portu UDP** i w polu **Port UDP** określ numer portu. Domyślnie opcja ta jest wyłączona i używany jest port TCP. Jeśli ta opcja jest włączona, domyślny port UDP do nawiązywania połączenia z serwerem KSN proxy to 15111.
7. Włącz opcję **Połącz podrzędne Serwery administracyjne z KSN przez główny Serwer administracyjny**.

   Jeśli ta opcja jest włączona, podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera KSN proxy. Jeśli ta opcja jest wyłączona, podrzędne Serwery administracyjne same łączą się z KSN. W tym przypadku zarządzane urządzenia używają podrzędnych Serwerów administracyjnych jako serwerów KSN proxy.

   Podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera proxy, jeśli w prawej części sekcji **Ustawienia KSN Proxy**, dostępnej we właściwościach podrzędnych Serwerów administracyjnych, zaznaczono pole **Użyj Serwera administracyjnego jako serwera proxy**.

8. Kliknij **OK**.

Ustawienia dostępu do KSN zostaną zapisane.

Możesz także skonfigurować dostęp punktu dystrybucji do KSN, na przykład, jeśli chcesz zmniejszyć obciążenie na Serwerze administracyjnym. Punkt dystrybucji działający jako serwer KSN proxy wysyła żądania KSN z zarządzanych urządzeń bezpośrednio do Kaspersky, bez używania Serwera administracyjnego.

W celu skonfigurowania dostępu punktu dystrybucji do Kaspersky Security Network (KSN):

1. Upewnij się, że punkt dystrybucji został przypisany ręcznie.
2. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
3. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
4. W oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.
5. Na liście wskaż punkt dystrybucji i kliknij przycisk **Właściwości**, aby otworzyć jego okno właściwości.
6. W oknie właściwości punktu dystrybucji, w sekcji **KSN Proxy** zaznacz **Dostęp do chmury KSN bezpośrednio przez internet**.
7. Kliknij **OK**.

Punkt dystrybucji będzie działał jako serwer KSN proxy.

Włączanie i wyłączanie KSN

W celu włączenia KSN:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz wyłączyć KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **KSN Proxy** wybierz podsekcję **Ustawienia KSN Proxy**.
4. Wybierz **Użyj Serwera administracyjnego jako serwera proxy**.

   Serwer KSN proxy zostanie włączony.
5. Zaznacz pole **Zgadzam się na korzystanie z Kaspersky Security Network**.

   Usługa KSN zostanie włączona.

   Jeśli ta opcja jest zaznaczona, urządzenia klienckie będą wysyłać wyniki instalacji łat do Kaspersky. Przed zaznaczeniem tego pola należy przeczytać i zaakceptować warunki Oświadczenia KSN.
6. Kliknij **OK**.

W celu wyłączenia KSN:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz wyłączyć KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.

3. W oknie właściwości Serwera administracyjnego, w sekcji **KSN Proxy** wybierz podsekcję **Ustawienia KSN Proxy**.
4. Odznacz pole **Użyj Serwera administracyjnego** jako serwera proxy, aby wyłączyć usługę KSN Proxy, lub odznacz pole **Zgadzam się na korzystanie z Kaspersky Security Network**.

   Jeśli ta opcja jest odznaczona, urządzenia klienckie nie będą wysyłać wyników instalacji łat do Kaspersky.

   Jeśli korzystasz z prywatnej sieci KSN, odznacz pole **Konfiguruj Private KSN**.

   Usługa KSN zostanie wyłączona.
5. Kliknij **OK**.

Przeglądanie zaakceptowanego Oświadczenia KSN

Po włączeniu Kaspersky Security Network (KSN) musisz przeczytać i zaakceptować Oświadczenie KSN. W każdej chwili możesz przejrzeć zaakceptowane Oświadczenie KSN.

W celu przejrzenia zaakceptowanego Oświadczenia KSN:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego włączyłeś KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **KSN Proxy** wybierz podsekcję **Ustawienia KSN Proxy**.
4. Kliknij odnośnik **Wyświetl zaakceptowane oświadczenie KSN**.

W otwartym oknie możesz przejrzeć treść zaakceptowanego Oświadczenia KSN.

Przeglądanie statystyk serwera proxy KSN

Serwer KSN proxy jest usługą ułatwiającą interakcję między infrastrukturą Kaspersky Security Network a urządzeniami klienckimi zarządzanymi przez Serwer administracyjny.

Korzystanie z serwera KSN proxy oferuje następujące możliwości:

- Urządzenia klienckie mogą wysyłać żądania do KSN oraz przesyłać informacje do KSN nawet wtedy, gdy nie mają bezpośredniego dostępu do internetu.
- Serwer KSN proxy buforuje przetwarzane dane, ograniczając obciążenie połączenia wychodzącego i czas oczekiwania na informacje żądane przez urządzenie klienckie.

W oknie właściwości Serwera administracyjnego możesz skonfigurować serwer KSN proxy i przejrzeć statystyki korzystania z serwera KSN proxy.

W celu przejrzenia statystyk dotyczących serwera proxy KSN:

1. Z drzewa konsoli wybierz Serwer administracyjny, dla którego chcesz przejrzeć statystyki KSN.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W oknie właściwości Serwera administracyjnego, w sekcji **KSN Proxy** wybierz podsekcję **Statystyki KSN Proxy**.

Ta sekcja wyświetla statystyki dotyczące działania serwera proxy KSN. Jeśli to konieczne, wykonaj dodatkowe działania:

- Kliknij **Odśwież**, aby zaktualizować statystyki korzystania z serwera KSN proxy.
- Kliknij przycisk **Eksportuj do pliku**, aby wyeksportować statystyki do pliku CSV.
- Kliknij przycisk **Sprawdź połączenie z KSN**, aby sprawdzić, czy Serwer administracyjny jest aktualnie połączony z KSN.

4. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.

Akceptowanie zaktualizowanego Oświadczenia KSN

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji lub uaktualniania Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz nadal korzystać z KSN zgodnie z wersją Oświadczenia KSN, którą zaakceptowałeś wcześniej.

Po aktualizacji lub uaktualnieniu Serwera administracyjnego zaktualizowane Oświadczenie KSN jest wyświetlane automatycznie. Jeśli odrzucisz zaktualizowane Oświadczenie KSN, nadal możesz je przejrzeć i zaakceptować później.

W celu wyświetlenia, a następnie zaakceptowania lub odrzucenia zaktualizowanego Oświadczenia KSN:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Na zakładce **Monitorowanie**, w sekcji **Monitorowanie** kliknij plik odnośnik **Zaakceptowane Oświadczenie Kaspersky Security Network jest nieaktualne**.

   Zostanie otwarte okno **Oświadczenie KSN**.
3. Uważnie przeczytaj Oświadczenie KSN, a następnie podejmij decyzję. Jeśli akceptujesz zaktualizowane Oświadczenie KSN, kliknij przycisk **Akceptuję warunki Umowy licencyjnej**. Jeśli odrzucisz zaktualizowane Oświadczenie KSN, kliknij przycisk **Anuluj**.

W zależności od Twojego wyboru KSN działa zgodnie z warunkami aktualnego lub zaktualizowanego Oświadczenia KSN. Możesz wyświetlić tekst zaakceptowanego Oświadczenia KSN we właściwościach Serwera administracyjnego w dowolnym momencie.

Udoskonalona ochrona przy pomocy Kaspersky Security Network

Kaspersky oferuje użytkownikom dodatkową warstwę ochrony przy pomocy Kaspersky Security Network. Ta metoda ochrony została zaprojektowana do walki z zaawansowanymi zagrożeniami i atakami zero-day. Zintegrowane technologie chmury oraz doświadczenie analityków wirusów z Kaspersky sprawiają, że Kaspersky Endpoint Security jest najlepszym wyborem, jeżeli chodzi o ochronę przed najbardziej wyszukanymi zagrożeniami sieci.

Szczegóły dotyczące udoskonalonej ochrony w Kaspersky Endpoint Security są dostępne na stronie Kaspersky.

Sprawdzanie, czy punkt dystrybucji działa jako serwer proxy KSN

Na zarządzanym urządzeniu przypisanym do pracy jako punkt dystrybucji możesz włączyć serwer proxy KSN. Zarządzane urządzenie działa jako serwer proxy KSN, gdy usługa ksnproxy jest uruchomiona na urządzeniu. Możesz lokalnie sprawdzić, włączyć lub wyłączyć tę usługę na urządzeniu.

Jako punkt dystrybucji można przypisać urządzenie z systemem Windows lub Linux. Metoda sprawdzania punktu dystrybucji zależy od systemu operacyjnego tego punktu dystrybucji.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Windows działa jako serwer proxy KSN:

1. Na urządzeniu punktu dystrybucji, w systemie Windows otwórz **Usługi** (**Wszystkie programy → Narzędzia administracyjne → Usługi**).

2. Na liście usług sprawdź, czy usługa ksnproxy jest uruchomiona.

   Jeśli usługa ksnproxy jest uruchomiona, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Jeśli chcesz, możesz wyłączyć usługę ksnproxy. W takim przypadku Agent sieciowy w punkcie dystrybucji przestaje uczestniczyć w Kaspersky Security Network. To działanie wymaga uprawnień administratora lokalnego.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Linux działa jako serwer proxy KSN:

1. Na urządzeniu punktu dystrybucji wyświetl listę uruchomionych procesów.

2. Na liście uruchomionych procesów sprawdź, czy proces `/opt/kaspersky/ksc64/sbin/ksnproxy` jest uruchomiony.

Jeśli proces `/opt/kaspersky/ksc64/sbin/ksnproxy` jest uruchomiony, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Przełączanie między pomocą online i pomocą offline

Jeśli nie masz dostępu do internetu, możesz skorzystać z pomocy offline.

W celu przełączenia między pomocą online i pomocą offline:

1. W oknie głównym Kaspersky Security Center, w drzewie konsoli wybierz **Kaspersky Security Center 14.2**.

2. Kliknij odnośnik **Globalne ustawienia interfejsu**.

   Zostanie otwarte okno ustawień.

3. W oknie ustawień kliknij **Użyj pomocy offline**.

4. Kliknij **OK**.

Ustawienia zostaną zastosowane i zapisane. Jeśli chcesz, możesz w dowolnym momencie wrócić do poprzednich ustawień i rozpocząć korzystanie z pomocy online.

Eksportowanie zdarzeń do systemów SIEM

Ta sekcja opisuje sposób eksportowania zdarzeń zarejestrowanych przez Kaspersky Security Center do zewnętrznych systemów SIEM (Security Information and Event Management).

Scenariusz: Konfigurowanie eksportowania zdarzeń do systemów SIEM

Kaspersky Security Center umożliwia konfigurowanie przy użyciu jednej z następujących metod: eksportowanie do dowolnego systemu SIEM korzystającego z formatu Syslog, eksportowanie do systemów QRadar, Splunk, ArcSight SIEM korzystających z formatów LEEF i CEF lub eksportowanie zdarzeń do systemów SIEM bezpośrednio z bazy danych Kaspersky Security Center. Po zakończeniu tego scenariusza Serwer administracyjny automatycznie wysyła zdarzenia do systemu SIEM.

Wymagania wstępne

Zanim rozpoczniesz konfigurowanie eksportowania zdarzeń w Kaspersky Security Center:

- Dowiedz się więcej o metodach eksportowania zdarzeń.
- Upewnij się, że posiadasz wartości ustawień systemowych.

Możesz wykonać kroki tego scenariusza w dowolnej kolejności.

Proces eksportowania zdarzeń do systemu SIEM obejmuje następujące kroki:

- **Konfigurowanie systemu SIEM do odbierania zdarzeń z Kaspersky Security Center**

  Instrukcja: Konfigurowanie eksportowania zdarzeń w systemie SIEM

- **Wybieranie zdarzeń, które chcesz wyeksportować do systemu SIEM:**

  Dostępne instrukcje:

  - Konsola administracyjna: Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog, Oznaczanie ogólnych zdarzeń do eksportowania w formacie Syslog
  - Kaspersky Security Center Web Console: Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog, Oznaczanie ogólnych zdarzeń do eksportowania w formacie Syslog

- **Konfigurowanie eksportowania zdarzeń do systemu SIEM za pomocą jednej z poniższych metod:**

  - Korzystanie z protokołów TCP/IP, UDP lub TLS przez protokoły TCP.

    Dostępne instrukcje:

    - Konsola administracyjna: Konfigurowanie eksportowania zdarzeń do systemów SIEM
    - Kaspersky Security Center Web Console: Konfigurowanie eksportowania zdarzeń do systemów SIEM

  - Używanie eksportowania zdarzeń bezpośrednio z bazy danych Kaspersky Security Center (zestaw widoków publicznych jest dostępny w bazie danych Kaspersky Security Center; opis tych widoków publicznych można znaleźć w dokumencie klakdb.chm).

Wyniki

Po skonfigurowaniu eksportowania zdarzeń do systemu SIEM możesz przeglądać eksportowanie wyników, jeśli wybrałeś zdarzenia, które chcesz wyeksportować.

Czynności niezbędne do wykonania przed rozpoczęciem pracy

Podczas konfigurowania automatycznego eksportowania zdarzeń w Kaspersky Security Center musisz określić niektóre ustawienia systemu SIEM. Zalecane jest wcześniejsze sprawdzenie tych ustawień w celu przygotowania do konfiguracji Kaspersky Security Center.

W celu pomyślnego skonfigurowania automatycznego wysyłania zdarzeń do systemu SIEM należy znać następujące ustawienia:

- **Adres serwera systemu SIEM**

  Adres IP serwera, na którym zainstalowany jest aktualnie używany system SIEM. Sprawdź wartość tego ustawienia w ustawieniach systemu SIEM.

- **Port serwera systemu SIEM**

  Numer portu używanego do nawiązania połączenia pomiędzy Kaspersky Security Center a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

- **Protokół**

  Protokół używany do przesyłania wiadomości z Kaspersky Security Center do Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

Informacje o zdarzeniach w Kaspersky Security Center

Kaspersky Security Center umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego. Możesz wyeksportować te informacje do zewnętrznych systemów SIEM. Eksportowanie informacji o zdarzeniach do zewnętrznych systemów SIEM umożliwia administratorom systemów SIEM natychmiastowe reagowanie na zdarzenia dotyczące systemu bezpieczeństwa, które pojawiają się na zarządzanych urządzeniach lub w grupach administracyjnych.

Typy zdarzeń

W Kaspersky Security Center dostępne są następujące typy zdarzeń:

- Zdarzenia ogólne. Te zdarzenia występują we wszystkich zarządzanych aplikacjach firmy Kaspersky. Przykładem zdarzenia ogólnego jest Epidemia wirusa. Zdarzenia ogólne mają dokładnie zdefiniowaną składnię i semantykę. Zdarzenia ogólne są używane, na przykład, w raportach i pulpitach nawigacyjnych.

- Zarządzane zdarzenia charakterystyczne dla aplikacji firmy Kaspersky. Każda zarządzana aplikacja firmy Kaspersky posiada swój zestaw zdarzeń.

Źródła zdarzeń

Zdarzenia mogą być generowane przez następujące aplikacje:

- Składniki Kaspersky Security Center:
  - Serwer administracyjny
  - Agent sieciowy
  - Serwer iOS MDM
  - Serwer urządzeń mobilnych Exchange
- Zarządzane aplikacje Kaspersky

  Szczegółowe informacje na temat zdarzeń generowanych przez aplikacje zarządzane przez Kaspersky można znaleźć w dokumentacji odpowiedniej aplikacji.

Możesz wyświetlić pełną listę zdarzeń, które mogą być generowane przez aplikację na karcie **Konfiguracja zdarzenia** w zasadzie aplikacji. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić listę zdarzeń we właściwościach Serwera administracyjnego.

Poziom ważności zdarzeń

Każde zdarzenie posiada priorytet. W zależności od warunków wystąpienia zdarzenia, może ono posiadać różne priorytety. Istnieją cztery priorytety zdarzeń:

- *Zdarzenie krytyczne* to zdarzenie, które wskazuje wystąpienie krytycznego problemu mogącego prowadzić do utraty danych, problemów z działaniem lub błędu krytycznego.
- *Błąd funkcjonalny* to zdarzenie, które wskazuje poważny problem, błąd lub problem z działaniem, który wystąpił podczas działania aplikacji lub podczas przeprowadzania procedury.
- *Ostrzeżenie* to zdarzenie, które niekoniecznie jest poważne, ale wskazuje możliwość wystąpienia potencjalnego problemu w przyszłości. Większość zdarzeń otrzymuje priorytet „Ostrzeżenie", jeśli aplikacja może zostać przywrócona bez utraty danych lub możliwości funkcyjnych aplikacji.
- *Informacja* to zdarzenie, którego celem jest informowanie o pomyślnym zakończeniu działania, właściwym funkcjonowaniu aplikacji lub zakończeniu procedury.

Każde zdarzenie posiada zdefiniowany okres przechowywania, w trakcie którego możesz przejrzeć lub zmodyfikować to zdarzenie w Kaspersky Security Center. Niektóre zdarzenia nie są domyślnie zapisywane w bazie danych Serwera administracyjnego, ponieważ ich zdefiniowany okres przechowywania wynosi zero. Tylko te zdarzenia, które będą przechowywane w bazie danych Serwera administracyjnego przynajmniej jeden dzień, mogą zostać wyeksportowane do systemów zewnętrznych.

Informacje o eksportowaniu zdarzeń

Eksportowanie zdarzeń może być używane w obrębie scentralizowanych systemów, które zajmują się problemami z bezpieczeństwem na poziomie organizacyjnym i technicznym, zapewniają usługi monitorowania ochrony oraz skonsolidowane informacje z różnych rozwiązań. To są systemy SIEM, które oferują przeprowadzania w czasie rzeczywistym analizy ostrzeżeń i zdarzeń zabezpieczeń, wygenerowanych przez aplikacje i sprzęt w sieci, lub Security Operation Centers (SOCs).

Te systemy otrzymują dane z wielu źródeł, w tym sieci, ochrony, serwerów, baz danych i aplikacji. Systemy SIEM oferują także funkcjonalność konsolidowania monitorowanych danych, aby pomóc w uniknięciu przeoczenia zdarzeń krytycznych. Dodatkowo, systemy przeprowadzają zautomatyzowaną analizę powiązanych zdarzeń i ostrzeżeń w celu powiadomienia administratorów o nagłych problemach z bezpieczeństwem. Wysyłanie ostrzeżeń może zostać zaimplementowane poprzez pulpit nawigacyjny lub wysyłanie ostrzeżeń może się odbywać poprzez kanały firm trzecich, na przykład pocztę elektroniczną.

Proces eksportowania zdarzeń z Kaspersky Security Center do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia – Kaspersky Security Center oraz odbiorca zdarzenia – system SIEM. Aby pomyślnie eksportować zdarzenia, należy skonfigurować tę funkcję w posiadanym systemie SIEM i w Konsoli administracyjnej Kaspersky Security Center. Nie ma znaczenia, która strona zostanie skonfigurowana jako pierwsza. Możesz skonfigurować przesyłanie zdarzeń w Kaspersky Security Center, a następnie skonfigurować odbieranie zdarzeń przez system SIEM lub na odwrót.

Metody wysyłania zdarzeń z Kaspersky Security Center

Dostępne są trzy metody wysyłania zdarzeń z Kaspersky Security Center do systemów zewnętrznych:

- Wysyłanie zdarzeń po protokole Syslog do dowolnego systemu SIEM

  Korzystając z protokołu Syslog, możesz przekazywać dowolne zdarzenia, które wystąpiły na Serwerze administracyjnym Kaspersky Security Center i w aplikacjach firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Możesz go użyć do eksportowania zdarzeń do systemu SIEM.

  W tym celu należy zaznaczyć zdarzenia, które chcemy przekazać do systemu SIEM. Możesz zaznaczyć zdarzenia w Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console. Tylko zaznaczone zdarzenia będą przekazywane do systemu SIEM. Jeśli nic nie zaznaczysz, żadne zdarzenia nie zostaną przekazane.

- Wysyłanie zdarzeń po protokołach CEF i LEEF do systemów QRadar, Splunk i ArcSight

  Możesz używać protokołów CEF i LEEF do eksportowania zdarzeń ogólnych. Podczas eksportowania zdarzeń po protokołach CEF i LEEF nie masz możliwości wyboru określonych zdarzeń do wyeksportowania. Eksportowane są wszystkie zdarzenia ogólne. W przeciwieństwie do protokołu Syslog, protokoły CEF i LEEF nie są uniwersalne. Protokoły CEF i LEEF są przeznaczone dla odpowiednich systemów SIEM (QRadar, Splunk i ArcSight). Dlatego też, jeśli wybierzesz eksportowanie zdarzeń poprzez jeden z tych protokołów, użyjesz parsera w systemie SIEM.

  > Aby wyeksportować zdarzenia poprzez protokoły CEF i LEEF, funkcja integracji z systemami SIEM musi być aktywowana w Serwerze administracyjnym przy użyciu aktywnego klucza licencyjnego lub ważnego kodu aktywacyjnego.

- Bezpośrednio z bazy danych Kaspersky Security Center do dowolnego systemu SIEM

  Ta metoda eksportowania zdarzeń może zostać użyta do odbierania zdarzeń bezpośrednio z widoków publicznych bazy danych przy użyciu zapytań SQL. Wyniki zapytań są zapisywane do pliku XML, który może zostać użyty jako dane wejściowe systemu zewnętrznego. Tylko zdarzenia dostępne w widokach publicznych mogą być eksportowane bezpośrednio z bazy danych.

Odbieranie zdarzeń przez system SIEM

System SIEM musi odbierać i poprawnie analizować zdarzenia otrzymywane z Kaspersky Security Center. W tym celu należy odpowiednio skonfigurować system SIEM. Konfiguracja zależy od specyfiki używanego systemu SIEM. Jednakże istnieje kilka ogólnych kroków w konfiguracji wszystkich systemów SIEM, takie jak konfigurowanie odbiorcy i analizatora.

Informacje o konfigurowaniu eksportowania zdarzeń w systemie SIEM

Proces eksportowania zdarzeń z Kaspersky Security Center do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia—Kaspersky Security Center oraz odbiorca zdarzenia—system SIEM. Należy skonfigurować eksportowanie zdarzeń w posiadanym systemie SIEM i w Kaspersky Security Center.

Ustawienia określane w systemie SIEM zależą od określonego systemu, którego używasz. Zazwyczaj dla wszystkich systemów SIEM należy skonfigurować odbiorcę i, opcjonalnie, analizatora wiadomości do analizowania otrzymanych zdarzeń.

Konfigurowanie odbiorcy

Aby otrzymywać zdarzenia wysyłane przez Kaspersky Security Center, należy skonfigurować odbiorcę w swoim systemie SIEM. W systemie SIEM powinny zostać określone następujące ustawienia:

- **Protokół eksportu lub typ wejścia**

  Jest to protokół obsługujący przesyłanie wiadomości - TCP/IP lub UDP. Ten protokół musi być taki sam, jak protokół, który określiłeś w Kaspersky Security Center.

- **Port**

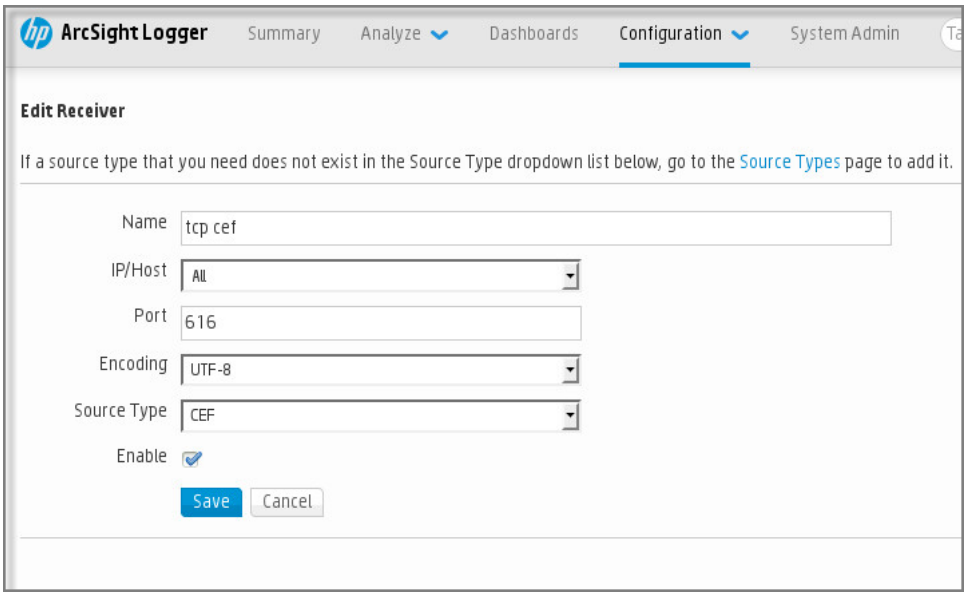
  Numer portu do nawiązana połączenia z Kaspersky Security Center. Ten port musi być taki sam, jak port, który określiłeś w Kaspersky Security Center.

- **Protokół wiadomości lub typ źródła**

  Protokół używany do eksportowania zdarzeń do systemu SIEM. Może to być jeden ze standardowych protokołów: Syslog, CEF lub LEEF. System SIEM wybiera analizatora wiadomości zgodnie z protokołem, który określiłeś.

W zależności od używanego systemu SIEM, konieczne może być określenie niektórych dodatkowych ustawień odbiorcy.

Poniższy rysunek przedstawia okno konfiguracji odbiorcy w ArcSight.



Konfiguracja odbiorcy w ArcSight

Analizator wiadomości

Wyeksportowane zdarzenia są przekazywane do systemu SIEM jako wiadomości. Te wiadomości muszą być odpowiednio przeanalizowane, aby informacje na temat zdarzeń mogły być użyte przez system SIEM. Analizatory wiadomości są częścią systemu SIEM; są używane do podzielenia zawartości wiadomości na odpowiednie pola, takie jak: ID zdarzenia, priorytet, opis, parametry itd. Umożliwia to systemowi SIEM przetworzenie zdarzeń otrzymanych z Kaspersky Security Center tak, aby mogły być przechowywane w bazie danych systemu SIEM.

Każdy system SIEM posiada zestaw standardowych analizatorów wiadomości. Kaspersky także dostarcza analizatory wiadomości dla niektórych systemów SIEM, na przykład dla QRadar i ArcSight. Te analizatory wiadomości można pobrać ze stron internetowych odpowiednich systemów SIEM. Podczas konfigurowania odbiorcy możesz wybrać używanie jednego ze standardowych analizatorów wiadomości lub analizatora wiadomości od Kaspersky.

Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog

W tej sekcji opisano, jak oznaczyć zdarzenia do dalszego eksportu do systemów SIEM w formacie Syslog.

Informacje dotyczące oznaczania zdarzeń do wyeksportowania do systemu SIEM w formacie Syslog

Po włączeniu automatycznego eksportowania zdarzeń, należy wskazać zdarzenia, które zostaną wyeksportowane do zewnętrznego systemu SIEM.

Możesz skonfigurować eksportowanie zdarzeń w formacie Syslog do zewnętrznego systemu w oparciu o jeden z następujących warunków:

- Oznaczanie zdarzeń ogólnych. Jeśli zdarzenia do wyeksportowania oznaczysz w zasadzie, w ustawieniach zdarzenia lub w ustawieniach Serwera administracyjnego system SIEM otrzyma oznaczone zdarzenia, które

wystąpiły we wszystkich aplikacjach zarządzanych przez określoną zasadę. Jeśli wyeksportowane zdarzenia były wybrane w profilu, nie będziesz mógł ich ponownie zdefiniować dla aplikacji zarządzanej przez ten profil.

- Oznaczanie zdarzeń dla zarządzanej aplikacji. Jeśli oznaczysz zdarzenia do wyeksportowania dla zarządzanej aplikacji, zainstalowanej na zarządzanym urządzeniu, system SIEM otrzyma tylko zdarzenia, które wystąpiły w tej aplikacji.

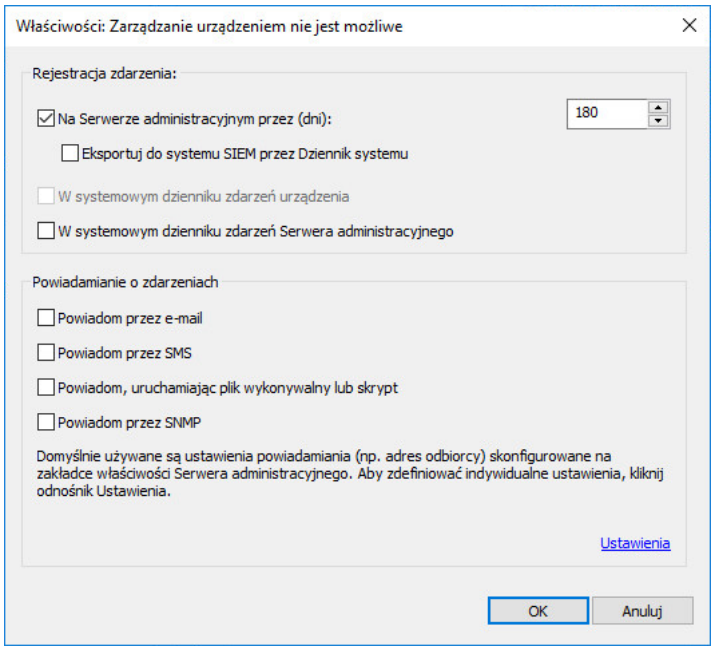
Oznaczanie zdarzeń aplikacji Kaspersky do eksportu w formacie Syslog

Jeśli chcesz wyeksportować zdarzenia, które wystąpiły w pojedynczej zarządzanej aplikacji, zainstalowanej na zarządzanym urządzeniu, dla aplikacji oznacz zdarzenia do wyeksportowania. Jeśli poprzednio wyeksportowane zdarzenia były oznaczone w zasadzie, nie będziesz mógł ponownie zdefiniować oznaczonych zdarzeń dla pojedynczej aplikacji zarządzanej przez tę zasadę.

W celu oznaczenia zdarzeń do wyeksportowania dla pojedynczej zarządzanej aplikacji:

1. W drzewie konsoli Kaspersky Security Center wybierz węzeł **Zarządzane urządzenia** i przejdź na zakładkę **Urządzenia**.
2. Kliknij żądane urządzenie prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.
3. W otwartym oknie właściwości urządzenia wybierz sekcję **Aplikacje**.
4. Na liście aplikacji, która zostanie wyświetlona, wybierz aplikację, której zdarzenia chcesz wyeksportować, i kliknij przycisk **Właściwości**.
5. W oknie właściwości aplikacji wybierz sekcję **Konfiguracja zdarzenia**.
6. Na liście zdarzeń, która zostanie wyświetlona, wybierz jedno lub kilka zdarzeń do wyeksportowania do systemu SIEM i kliknij przycisk **Właściwości**.
7. W wyświetlonym oknie właściwości zdarzeń zaznacz pole **Eksportuj do systemu SIEM przez Dziennik systemu**, aby zaznaczyć wybrane zdarzenia do eksportu w formacie Syslog. Odznacz pole **Eksportuj do systemu SIEM przez Dziennik systemu** wyboru, aby odznaczyć wybrane zdarzenia do eksportu w formacie Syslog.

   Jeśli właściwości zdarzenia są zdefiniowane w profilu, pola w tym oknie nie mogą być modyfikowane.



Okno Właściwości zdarzenia

8. Kliknij **OK**, aby zachować zmiany.

9. Kliknij **OK** w oknie właściwości aplikacji i w oknie właściwości urządzenia.

Wybrane zdarzenia zostaną wysłane do systemu SIEM w formacie Syslog. Wydarzenia, dla których odznaczyłeś pole **Eksportuj do systemu SIEM przez Dziennik systemu**, nie zostaną wyeksportowane do systemu SIEM. Proces eksportowania rozpocznie się natychmiast po włączeniu automatycznego eksportowania i wybraniu zdarzeń do wyeksportowania. Skonfiguruj system SIEM, aby mógł otrzymywać zdarzenia z Kaspersky Security Center.

Oznaczanie ogólnych zdarzeń do eksportu w formacie Syslog

Jeśli chcesz wyeksportować zdarzenia, które wystąpiły we wszystkich aplikacjach zarządzanych przez określoną zasadę, w zasadzie wybierz zdarzenia do wyeksportowania. W tym przypadku nie będziesz mógł wybrać zdarzeń dla pojedynczej zarządzanej aplikacji.

W celu oznaczenia zdarzeń ogólnych do wyeksportowania do systemu SIEM:

1. W drzewie konsoli Kaspersky Security Center wybierz węzeł **Zasady**.

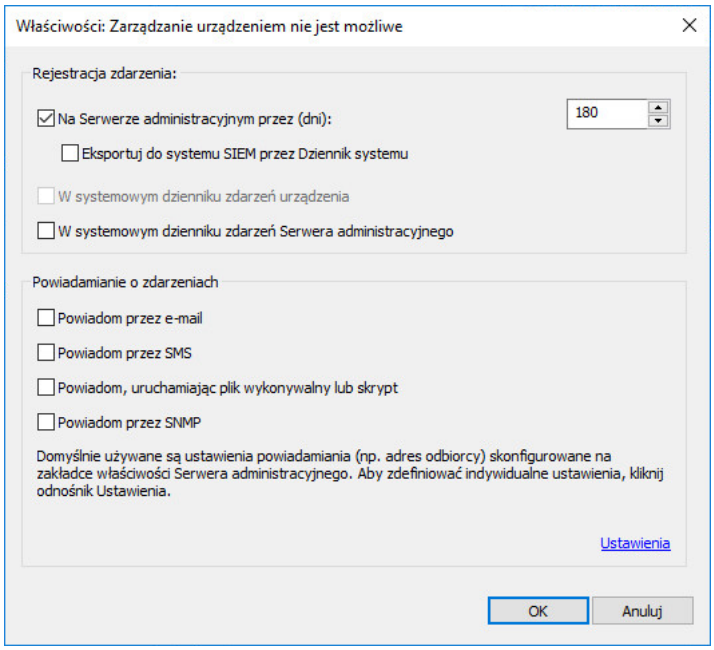
2. Kliknij żądany profil prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Właściwości**.

3. W otwartym oknie właściwości profilu wybierz sekcję **Konfiguracja zdarzenia**.

4. Na liście zdarzeń, która zostanie wyświetlona, wybierz jedno lub kilka zdarzeń do wyeksportowania do systemu SIEM i kliknij przycisk **Właściwości**.

   Jeśli chcesz wybrać wszystkie zdarzenia, kliknij przycisk **Wybierz wszystkie**.

5. W wyświetlonym oknie właściwości zdarzeń zaznacz pole **Eksportuj do systemu SIEM przez Dziennik systemu**, aby zaznaczyć wybrane zdarzenia do eksportu w formacie Syslog. Odznacz pole **Eksportuj do systemu SIEM przez Dziennik systemu**, aby odznaczyć wybrane zdarzenia do eksportu w formacie Syslog.



Okno właściwości zdarzenia Serwera administracyjnego

6. Kliknij **OK**, aby zachować zmiany.

7. W oknie właściwości profilu kliknij **OK**.

Wybrane zdarzenia zostaną wysłane do systemu SIEM w formacie Syslog. Wydarzenia, dla których odznaczyłeś pole **Eksportuj do systemu SIEM przez Dziennik systemu**, nie zostaną wyeksportowane do systemu SIEM. Proces eksportowania rozpocznie się natychmiast po włączeniu automatycznego eksportowania i wybraniu zdarzeń do wyeksportowania. Skonfiguruj system SIEM, aby mógł otrzymywać zdarzenia z Kaspersky Security Center.

Informacje dotyczące eksportowania zdarzeń przy użyciu formatu Syslog

Możesz użyć formatu Syslog do wyeksportowania do systemów SIEM zdarzeń, które występują na Serwerze administracyjnym i w innych aplikacjach firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach.

Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Pozwala on na rozdzielenie oprogramowania, które generuje wiadomości, systemu, które je przechowuje, oraz oprogramowania, które raportuje i analizuje te wiadomości. Do każdej wiadomości przypisywany jest kod funkcji, wskazujący typ oprogramowania, które generuje wiadomość, oraz priorytet.

Format Syslog jest definiowany przez dokumenty RFC (Request for Comments — prośba o komentarze), publikowane przez Internet Engineering Task Force (standardy internetowe). Standard RFC 5424 jest używany do eksportowania zdarzeń z Kaspersky Security Center do systemów zewnętrznych.

W Kaspersky Security Center możesz skonfigurować eksportowanie zdarzeń do systemów zewnętrznych przy użyciu formatu Syslog.

Proces eksportowania składa się z dwóch etapów:

1. Włączanie automatycznego eksportowania zdarzeń. W tym kroku program Kaspersky Security Center jest konfigurowany tak, aby wysyłał zdarzenia do systemu SIEM. Kaspersky Security Center rozpoczyna wysyłanie zdarzeń natychmiast po włączeniu automatycznego eksportowania.

2. Wybieranie zdarzeń eksportowanych do systemu zewnętrznego. W tym kroku wybierasz zdarzenia, które będą eksportowane do systemu SIEM.

Informacje dotyczące eksportowania zdarzeń przy użyciu formatów CEF i LEEF

Możesz użyć formatów CEF i LEEF, aby wyeksportować ogólne zdarzenia do systemów SIEM, a także zdarzenia przesyłane przez aplikacje Kaspersky do Serwera administracyjnego. Zestaw eksportowanych zdarzeń jest predefiniowany i nie możesz wybrać zdarzeń do wyeksportowania.

Aby wyeksportować zdarzenia poprzez protokoły CEF i LEEF, funkcja integracji z systemami SIEM musi być aktywowana w Serwerze administracyjnym przy użyciu aktywnego klucza licencyjnego lub ważnego kodu aktywacyjnego.

Wybierz format eksportowania w oparciu o używany system SIEM. Poniższa tabela wyświetla systemy SIEM i odpowiadające im formaty eksportu.

Formaty eksportowania zdarzenia do systemu SIEM

System SIEM	Format eksportu
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - dostosowany format zdarzeń dla IBM Security QRadar SIEM. QRadar może integrować, identyfikować i przetwarzać zdarzenia LEEF. Zdarzenia LEEF muszą używać kodowania UTF-8. Szczegółowe informacje na temat protokołu LEEF można znaleźć w Centrum wiedzy IBM.

- CEF (Common Event Format)—standard zarządzania dziennikami, który ulepsza współdziałanie zdarzeń dotyczących bezpieczeństwa między różnymi urządzeniami i aplikacjami sieciowymi i zabezpieczającymi. CEF umożliwia korzystanie z podstawowego formatu dziennika zdarzeń, co ułatwia integrowanie i gromadzenie danych do analizy przez system zarządzania korporacji.

Automatyczne eksportowanie oznacza, że Kaspersky Security Center wysyła ogólne zdarzenia do systemu SIEM. Automatyczne eksportowanie zdarzeń rozpoczyna się od razu po włączeniu tej opcji. Ta sekcja szczegółowo wyjaśnia, jak włączyć automatyczne eksportowanie zdarzeń.

Konfigurowanie Kaspersky Security Center do wyeksportowania zdarzeń do systemu SIEM

Możesz włączyć automatyczne eksportowanie zdarzeń w Kaspersky Security Center.

Tylko zdarzenia ogólne mogą być eksportowane z zarządzanych aplikacji w formatach CEF i LEEF. Zdarzenia specyficzne dla aplikacji nie mogą być eksportowane z zarządzanych aplikacji w formatach CEF i LEEF. Jeśli chcesz wyeksportować zdarzenia zarządzanych aplikacji lub niestandardowy zestaw zdarzeń, który został skonfigurowany przy użyciu zasad zarządzanych aplikacji, wyeksportuj zdarzenia w formacie Syslog.

W celu włączenia automatycznego eksportowania zdarzeń:

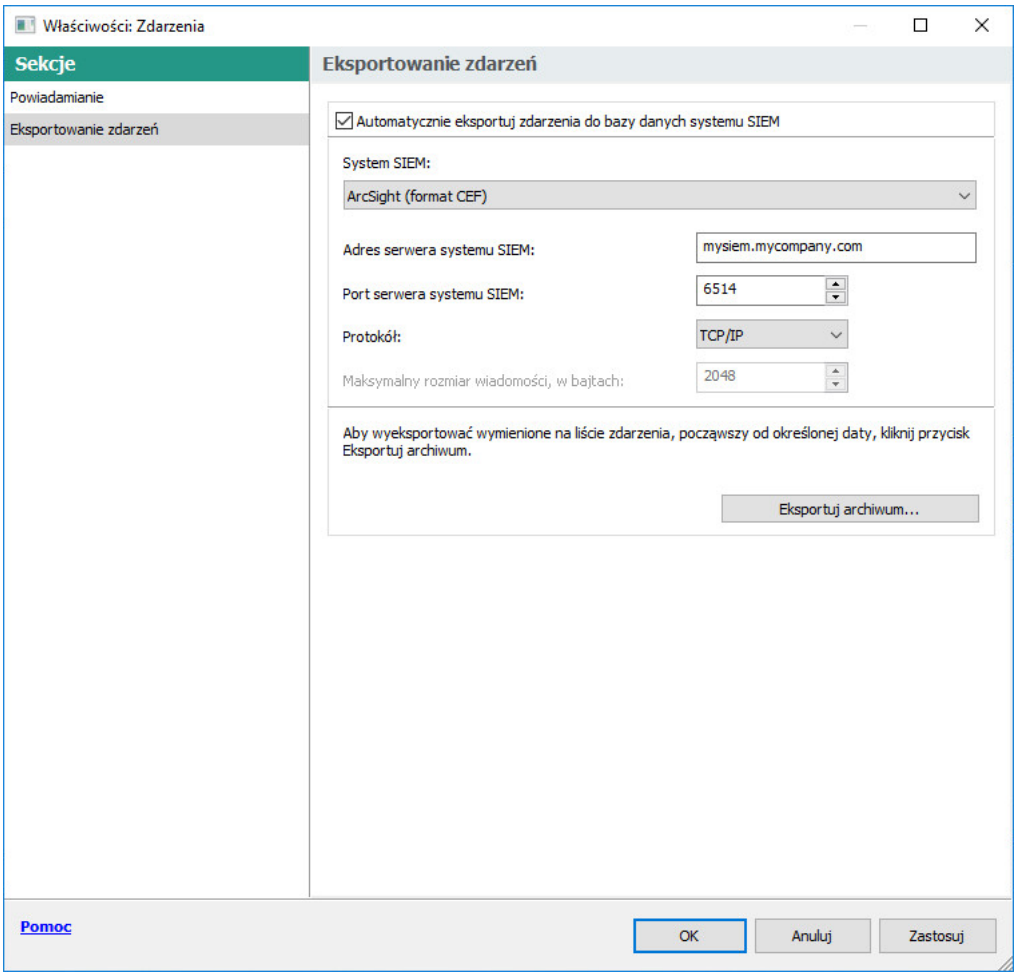
1. W drzewie konsoli Kaspersky Security Center wybierz Serwer administracyjny, którego zdarzenia chcesz wyeksportować.

2. W obszarze roboczym wybranego Serwera administracyjnego wybierz zakładkę **Zdarzenia**.

3. Kliknij strzałkę rozwijalną znajdującą się obok odnośnika **Konfiguruj powiadomienia i eksportowanie zdarzeń** i z listy rozwijalnej wybierz **Konfiguruj eksportowanie do SIEM**.

   Okno właściwości zdarzeń zostanie otwarte na sekcji **Eksportowanie zdarzeń**.

4. W sekcji **Eksportowanie zdarzeń** określ następujące ustawienia eksportowania:



Sekcja Eksportowanie zdarzeń w oknie właściwości zdarzeń

- Automatycznie eksportuj zdarzenia do bazy danych systemu SIEM

  Zaznacz to pole, aby włączyć automatyczne eksportowanie zdarzeń do systemów SIEM. Zaznaczenie tego pola włącza wszystkie pola w sekcji **Eksportowanie zdarzeń**.

- System SIEM

  Wybierz system SIEM, do którego zostaną wyeksportowane zdarzenia: QRadar® (format LEEF), ArcSight (format CEF), Splunk® (format CEF) i format Syslog (RFC 5424).

- Adres serwera systemu SIEM

  Określ adres serwera systemu SIEM. Adres można określić jako nazwę DNS lub NetBIOS lub jako adres IP.

- **Port serwera systemu SIEM**

  Określ numer portu używanego do nawiązywania połączenia z serwerem systemu SIEM. Ten numer portu musi być taki sam, jak ten, którego Twój system SIEM używa do pobierania zdarzeń (więcej informacji można znaleźć w sekcji Konfigurowanie systemu SIEM).

- **Protokół**

Wybierz protokół, który będzie używany do przesyłania wiadomości do systemu SIEM. Możesz wybrać protokół TCP/IP, UDP lub TLS przez protokół TCP.

Określ następujące ustawienia TLS, jeśli wybierzesz TLS poprzez protokół TCP:

- **Uwierzytelnianie serwera SIEM**

  Wybierz jeden z poniższych sposobów uwierzytelnienia serwera systemu SIEM:

  - **Używając certyfikatów urzędu certyfikacji** Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji (CA) i przesłać go do Kaspersky Security Center. Kaspersky Security Center sprawdza, czy certyfikat serwera systemu SIEM jest również podpisany przez zaufany urząd certyfikacji, czy nie.

    Aby dodać zaufany certyfikat, kliknij przycisk **Przeglądaj**, a następnie prześlij certyfikat.

    W przypadku wybrania opcji **Używając certyfikatów urzędu certyfikacji** można określić nazwy podmiotów w polu **Podmioty certyfikatów serwera (opcjonalnie)**. *Nazwa podmiotu* to nazwa domeny, dla której otrzymano certyfikat. Kaspersky Security Center nie może połączyć się z serwerem systemu SIEM, jeśli nazwa domeny serwera systemu SIEM nie jest zgodna z nazwą podmiotu certyfikatu serwera systemu SIEM. Jednak serwer systemu SIEM może zmienić swoją nazwę domeny, jeśli zmienisz nazwę w certyfikacie. W tym celu określ nazwy podmiotów w polu **Podmioty certyfikatów serwera (opcjonalnie)** (opcjonalnie). Jeśli dowolna z podanych nazw podmiotów odpowiada nazwie podmiotu certyfikatu systemu SIEM, Kaspersky Security Center zweryfikuje certyfikat serwera systemu SIEM.

  - **Korzystając z odcisków palców SHA-1 certyfikatów serwera** Możesz określić odciski palców SHA-1 certyfikatów systemu SIEM w Kaspersky Security Center. Aby dodać odcisk palca SHA-1, wprowadź go w polu pod opcją.

- **Uwierzytelnianie klienta**

  W celu uwierzytelnienia klienta możesz wstawić swój certyfikat lub wygenerować go w Kaspersky Security Center.

  - **Wstaw certyfikat**. Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Aby wstawić istniejący certyfikat, kliknij przycisk **Wybierz certyfikat**. W otwartym oknie **Certyfikat** wybierz jeden z poniższych typów certyfikatów, a następnie określ certyfikat i jego klucz prywatny:

    - **Certyfikat X.509**. Prześlij plik z kluczem prywatnym w polu **Klucz prywatny (*.prk, *.pem)** oraz plik z certyfikatem w polu **Certyfikat(*.cer)**. W tym celu kliknij przycisk **Przeglądaj** po prawej stronie odpowiedniego pola, a następnie dodaj wymagany plik. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po przesłaniu obu plików określ hasło do dekodowania klucza prywatnego w polu **Hasło**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

    - **Kontener PKCS #12**. Prześlij pojedynczy plik zawierający certyfikat i jego klucz prywatny w polu **Plik certyfikatu**. W tym celu kliknij przycisk **Przeglądaj** po prawej stronie odpowiedniego pola, a następnie dodaj wymagany plik. Po przesłaniu pliku określ hasło do dekodowania klucza prywatnego w polu **Hasło**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

  - **Wygeneruj klucz**. Możesz wygenerować certyfikat z podpisem własnym w Kaspersky Security Center. Kliknij przycisk **Wygeneruj certyfikat**, a następnie wprowadź nazwę podmiotu w polu **Temat**. Certyfikat klienta jest generowany dla tej nazwy podmiotu, a odcisk palca SHA-1 tego certyfikatu jest wyświetlany w polu **Odcisk palca SHA-1 certyfikatu klienta**. W rezultacie Kaspersky Security Center przechowuje wygenerowany samopodpisany certyfikat i możesz przekazać publiczną część certyfikatu lub odcisk palca SHA-1 do systemu SIEM.

Jeśli wybierzesz format Syslog, musisz określić:

- **Maksymalny rozmiar wiadomości, w bajtach**

  Określ maksymalny rozmiar (w bajtach) jednej wiadomości przekazywanej do systemu SIEM. Każde zdarzenie jest przesyłane w jednej wiadomości. Jeśli rzeczywisty rozmiar wiadomości przekracza określoną wartość, wiadomość jest skracana i dane mogą zostać utracone. Domyślny rozmiar to 2048 bajtów. To pole jest dostępne tylko wtedy, gdy w polu **System SIEM** wybrałeś format dziennika systemu.

5. Jeśli chcesz wyeksportować do bazy danych systemu SIEM zdarzenia, które wystąpiły po określonej dacie w przeszłości, kliknij przycisk **Eksportuj archiwum** i określ datę początkową dla eksportowania zdarzeń. Domyślnie, eksportowanie zdarzeń rozpoczyna się od razu po włączeniu tej opcji.

6. Kliknij **OK**.

Automatyczne eksportowanie zdarzeń jest włączone.

Po włączeniu automatycznego eksportowania zdarzeń, należy wskazać zdarzenia, które zostaną wyeksportowane do systemu SIEM.

Eksportowanie zdarzeń bezpośrednio z bazy danych

Zdarzenia można otrzymywać bezpośrednio z bazy danych Kaspersky Security Center bez konieczności korzystania z interfejsu Kaspersky Security Center. Możesz wykonać zapytanie bezpośrednio do widoków publicznych i pobrać dane zdarzenia lub utworzyć swoje własne widoki w oparciu o istniejące widoki publiczne i adresować je w celu otrzymania żądanych danych.

Widoki publiczne

Dla Twojej wygody, w bazie danych Kaspersky Security Center dostępny jest zestaw widoków publicznych. Opis tych widoków publicznych można znaleźć w dokumentacji klakdb.chm.

Widok publiczny v_akpub_ev_event zawiera zestaw pól, które reprezentują parametry zdarzenia w bazie danych. W dokumencie klakdb.chm możesz także znaleźć informacje dotyczące widoków publicznych odpowiadających innym obiektom Kaspersky Security Center, na przykład: urządzeniom, aplikacjom lub użytkownikom. Możesz użyć tych informacji w swoich zapytaniach.

Ta sekcja zawiera instrukcje dotyczące tworzenia zapytania SQL przy użyciu narzędzia klsql2 oraz przykłady zapytań.

Aby utworzyć zapytania SQL lub widoki bazy danych, możesz także użyć innego dowolnego programu do pracy z bazami danych. Informacje dotyczące przeglądania parametrów połączenia z bazą danych Kaspersky Security Center, takich jak nazwa instancji i nazwa bazy danych, znajdują się w odpowiedniej sekcji.

Tworzenie zapytania SQL przy użyciu narzędzia klsql2

Ta sekcja opisuje sposób pobierania i korzystania z narzędzia klsql2, a także sposób tworzenia zapytań SQL przy użyciu tego narzędzia.

W celu pobrania i użycia narzędzia klsql2:

1. Pobierz narzędzie klsql2 ze strony internetowej Kaspersky. Nie używaj wersji narzędzia klsql2 przeznaczonych dla starszych wersji Kaspersky Security Center.

2. Skopiuj i rozpakuj pobrany plik klsql2.zip do dowolnego folderu na urządzeniu z zainstalowanym Serwerem administracyjnym Kaspersky Security Center.

   Pakiet klsql2.zip zawiera następujące pliki:

   - klsql2.exe
   - src.sql
   - start.cmd

3. Otwórz plik src.sql w dowolnym edytorze tekstu.

4. W pliku src.sql wpisz typ żądanego zapytania SQL, a następnie zapisz plik.

5. Na urządzeniu z zainstalowanym Serwerem administracyjnym Kaspersky Security Center, w wierszu polecenia wpisz następujące polecenie do uruchomienia zapytania SQL z pliku src.sql i zapisz wyniki do pliku result.xml:

   ```
   klsql2 -i src.sql -u <nazwa użytkownika> -p <hasło> -o result.xml
   ```

   gdzie `< nazwa użytkownika >` i `< hasło >` to poświadczenia konta użytkownika, który ma dostęp do bazy danych.

6. W razie potrzeby wprowadź login i hasło konta użytkownika, który ma dostęp do bazy danych.

7. Otwórz nowo utworzony plik result.xml, aby wyświetlić wyniki zapytania SQL.

Możesz zmodyfikować plik src.sql i utworzyć dowolne zapytanie SQL do widoków publicznych. Następnie, z poziomu wiersza poleceń, wykonaj zapytanie SQL i zapisz wyniki do pliku.

Przykład zapytania SQL w narzędziu klsql2

W tej sekcji przedstawiono przykład zapytania SQL, utworzonego przy użyciu narzędzia klsql2.

Poniższy przykład ilustruje otrzymanie zdarzeń, które wystąpiły na urządzeniach w ciągu ostatnich siedmiu dni, oraz wyświetlenie zdarzeń według czasu ich wystąpienia (najnowsze są wyświetlane jako pierwsze).

Na przykład:

```
SELECT
e.nId, /* identyfikator zdarzenia */
e.tmRiseTime, /* godzina wystąpienia zdarzenia */
e.strEventType, /* wewnętrzna nazwa typu zdarzenia */
e.wstrEventTypeDisplayName, /* wyświetlona nazwa zdarzenia */
e.wstrDescription, /* wyświetlony opis zdarzenia */
e.wstrGroupName, /* nazwa grupy, w której znajduje się zdarzenie */
h.wstrDisplayName, /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* adres IP urządzenia, na którym
wystąpiło zdarzenie */
FROM v_akpub_ev_event e
```

```
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Sprawdzanie nazwy bazy danych Kaspersky Security Center

Znajomość nazwy bazy danych może być pomocna, jeśli na przykład trzeba wysłać zapytanie SQL i połączyć się z bazą danych z edytora skryptów SQL.

W celu wyświetlenia nazwy bazy danych Kaspersky Security Center:

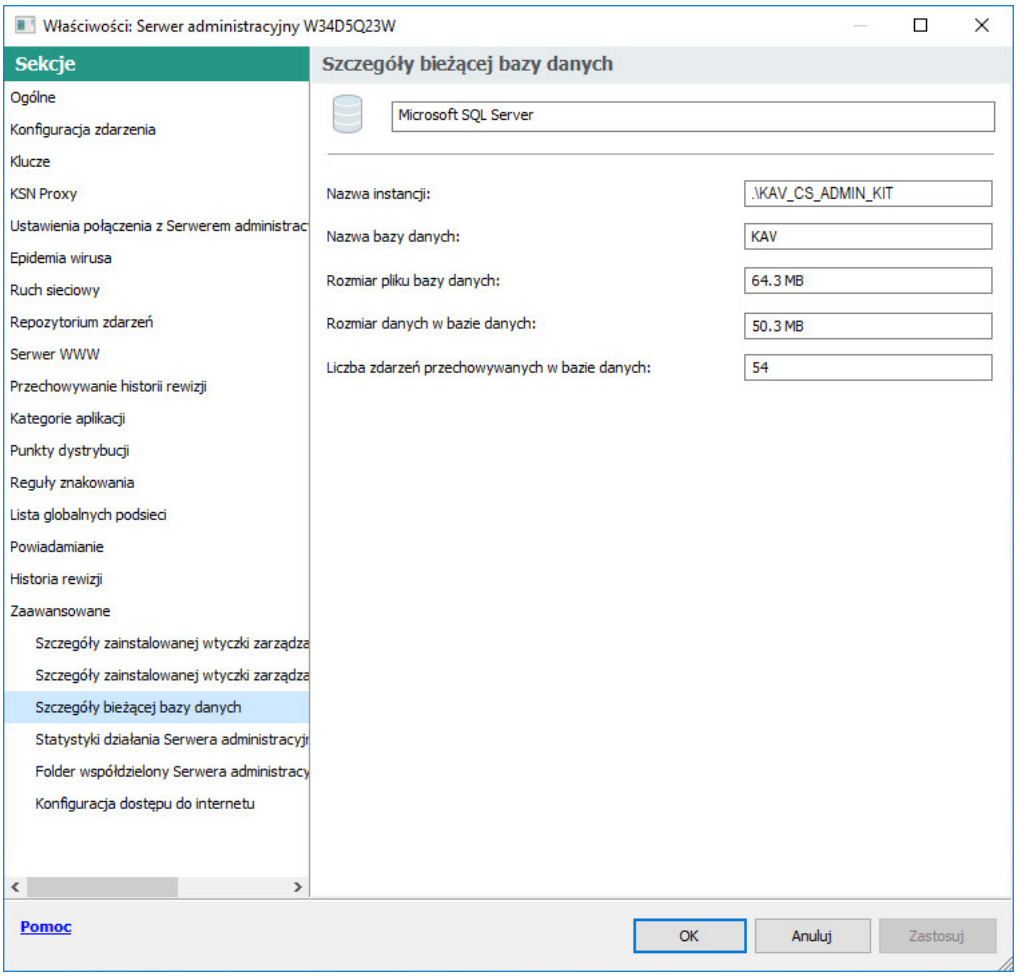
1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu Sekcje wybierz **Zaawansowane**, a następnie **Szczegóły bieżącej bazy danych**.
3. W sekcji **Szczegóły bieżącej bazy danych** zwróć uwagę na następujące właściwości bazy danych (patrz rysunek poniżej):

   - Nazwa instancji

     Nazwa bieżącej instancji bazy danych Kaspersky Security Center. Domyślna wartość to *.\KAV_CS_ADMIN_KIT*.

   - Nazwa bazy danych

     Nazwa bazy danych SQL Kaspersky Security Center. Domyślna wartość to *KAV*.



Sekcja z informacjami o bieżącej bazie danych Serwera administracyjnego

4. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.

Użyj nazwy bazy danych, aby adresować bazę danych w swoich zapytaniach SQL.

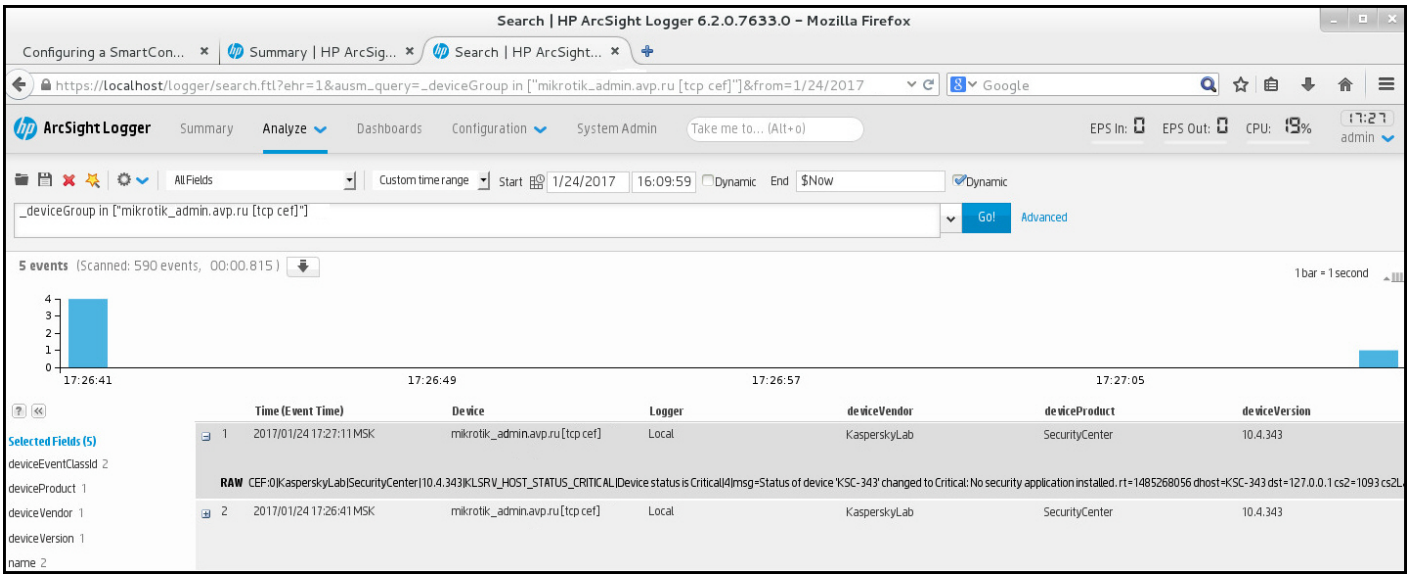
Przeglądanie wyników eksportowania

Możesz kontrolować pomyślne zakończenie procedury eksportowania zdarzeń. W tym celu sprawdź, czy wiadomości z eksportowanymi zdarzeniami są otrzymywane przez Twój system SIEM.

Jeśli zdarzenia wysłane z Kaspersky Security Center są odbierane i poprawnie analizowane przez Twój system SIEM, konfiguracja po obu stronach została przeprowadzona właściwie. Jeśli jest inaczej, sprawdź ustawienia, które określiłeś w Kaspersky Security Center, porównując je z konfiguracją w Twoim systemie SIEM.

Poniższy rysunek przedstawia zdarzenia wyeksportowane do ArcSight. Na przykład, pierwsze zdarzenie jest krytycznym zdarzeniem Serwera administracyjnego: „*Urządzenie posiada stan Krytyczny*”.

Reprezentacja eksportowania zdarzeń w systemie SIEM różni się w zależności od tego, którego systemu SIEM używasz.



Przykład zdarzeń

Używanie protokołu SNMP do wysyłania statystyk do aplikacji firm trzecich

Ta sekcja opisuje sposób pobierania informacji z Serwera administracyjnego przy użyciu protokołu SNMP (Simple Network Management Protocol) w systemie Windows. Kaspersky Security Center zawiera agenta SNMP, który przesyła statystyki działania Serwera administracyjnego do innych aplikacji przy użyciu identyfikatorów OID.

Ta sekcja zawiera również informacje o rozwiązywaniu problemów, które można napotkać podczas używania protokołu SNMP w przypadku Kaspersky Security Center.

Agent SNMP i identyfikatory obiektów

W przypadku Kaspersky Security Center agent SNMP jest zaimplementowany jako dynamiczna biblioteka `klsnmpag.dll`, która jest rejestrowana przez instalator podczas instalacji Serwera administracyjnego. Agent SNMP działa w procesie `snmp.exe` (jest to usługa systemu Windows). Aplikacje firm trzecich używają protokołu SNMP do odbierania statystyk (w postaci liczników) dotyczących działania Serwera administracyjnego.

Każdy licznik ma unikatowy *identyfikator obiektu* (nazywany również OID). Identyfikator obiektu to sekwencja liczb podzielonych kropkami. Identyfikatory obiektów Serwera administracyjnego zaczynają się od przedrostka 1.3.6.1.4.1.23668.1093. Identyfikator OID licznika jest połączeniem tego prefiksu z sufiksem opisującym licznik. Na przykład licznik o wartości OID 1.3.6.1.4.1.23668.1093.1.1.4 ma sufiks o wartości 1.1.4.

Możesz użyć klienta SNMP (takiego jak Zabbix) do monitorowania stanu Twojego systemu. Aby uzyskać informacje, możesz wyszukać wartość OID, która odpowiada informacjom i wprowadzić tę wartość do klienta SNMP. Wówczas Twój klient SNMP zwróci inną wartość, która charakteryzuje stan Twojego systemu.

Lista liczników i typów liczników znajduje się w pliku `adminkit.mib` na Serwerze administracyjnym. *MIB* to skrót od Management Information Base (baza informacji zarządzania). Pliki `.mib` można importować i analizować za pomocą aplikacji MIB Viewer, która służy do wysyłania zapytań o wartości liczników i ich wyświetlania.

Uzyskiwanie nazwy licznika ciągu znaków z identyfikatora obiektu

Aby użyć identyfikatora obiektu (OID) do przesyłania informacji do aplikacji firm trzecich, konieczne może być uzyskanie nazwy licznika ciągu znaków z tego identyfikatora obiektu.

W celu uzyskania nazwy licznika ciągu znaków z identyfikatora obiektu:

1. Otwórz plik `adminkit.mib`, który znajduje się na Serwerze administracyjnym, w edytorze tekstu.
2. Znajdź przestrzeń nazw opisującą pierwszą wartość (od lewej do prawej).

   Na przykład, dla sufiksu identyfikatora OID 1.1.4 będzie to `"counters" (::= { kladminkit 1 })`.
3. Znajdź przestrzeń nazw opisującą drugą wartość.

   Na przykład, dla sufiksu identyfikatora OID 1.1.4 będzie to `counters 1`, co oznacza `deployment`.
4. Znajdź przestrzeń nazw opisującą trzecią wartość.

   Na przykład, dla sufiksu identyfikatora OID 1.1.4 będzie to `deployment 4`, co oznacza `hostsWithAntivirus`.

Nazwa licznika ciągu znaków to połączenie tych wartości, na przykład `<MIB base namespace>.counters.deployment.hostsWithAntivirus` i odpowiada on identyfikatorowi OID o wartości 1.3.6.1.4.1.23668.1093.1.1.4.

Wartości identyfikatorów obiektów dla SNMP

Poniższa tabela przedstawia wartości i opisy identyfikatorów obiektów (OID), które są używane do przesyłania informacji o działaniu Serwera administracyjnego do aplikacji firm trzecich.

Wartości i opisy identyfikatorów obiektów dla SNMP

Wartość identyfikatora obiektu	Typ danych numerycznych	Identyfikator OID	Opis
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	Stan wdrożenia. Stan może być jednym z następujących: • **Informacja**. Licencja nie jest już ważna dla N urządzeń. • **Ostrzeżenie**. Jeden z następujących: Istnieje M urządzeń z aplikacjami Kaspersky zainstalowanymi na łącznie N urządzeniach w grupach Serwera administracyjnego (N > M). Licencja L utraci ważność na N urządzeniach za M dni. Zadanie T instalacji aplikacji zostało pomyślnie zakończone na N urządzeniach, dla M urządzeń konieczne jest ponowne uruchomienie. • **Krytyczne**. Licencja utraciła ważność dla N urządzeń.

			• **OK**. Żadne z powyższych.
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	Przyczyna, dla której stan deploymentStatus wskazuje, że grupa Serwera administracyjnego zawiera zbyt wiele urządzeń bez zarządzanyc aplikacji. Wartość jest równa 1 w przypadku wykrycia kilku urządzeń bez zarządzanych aplikacji, i 0 w innym przypadku
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	Przyczyna, dla której stan deploymentStatus wskazuje, że zadanie zdalnej instalacji nie powiodło się na niektórych urządzeniach. Liczbę tych urządzeń można uzyskać za pośrednictwem wartości hostsRemoteInstallFailed
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	Przyczyna, dla której stan deploymentStatus wskazuje, że istnieją urządzenia, dla których licencja utraci ważność w ciągu następnych 7 dni. Liczb tych urządzeń można uzyskać z pośrednictwem wartości hostsLicenseExpiring.
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	Przyczyna, dla której stan deploymentStatus wskazuje, że istnieją urządzenia z licencją która utraciła ważność. Liczbę tych urządzeń można uzyskać z pośrednictwem hostsLicenseExpired.
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	Liczba urządzeń w grupach Serwera administracyjnego.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	Liczba urządzeń w grupach Serwera administracyjnego z zainstalowanymi zarządzanymi aplikacjami.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	Liczba urządzeń, na których zadanie zdalnej instalacji nie powiodło się.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	Identyfikator klucza licencyjneg który wkrótce utraci ważność (mniej niż 7 dni).
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	Identyfikator wygasłego klucza licencyjnego.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	Liczba dni pozostałych do utra ważności licencji.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	Liczba urządzeń z licencją, któr

			wkrótce wygaśnie (za mniej niż dni).
`hostsLicenceExpired`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.10	Liczba urządzeń z licencją, któr utraciła ważność.
`updatesStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.2.1	Aktualny stan antywirusowych baz danych. Stan może być jednym z następujących: • **Informacja**. Serwer administracyjny nie był aktualizowany od więcej niż dnia, a od instalacji aplikacji minął mniej niż 1 dzień. • **Ostrzeżenie**. Serwer administracyjny nie był aktualizowany od więcej niż dnia. • **Krytyczne**. Serwer administracyjny nie był aktualizowany od ponad 2 d • **OK**. Żadne z powyższych.
`serverNotUpdated`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.1	Ta przyczyna wskazuje, że Serwer administracyjny nie był aktualizowany przez długi czas. Okres uważany za długi jest określony w wartości `updatesStatus`.
`notUpdatedHosts`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.2	Ta przyczyna wskazuje, że niektóre urządzenia nie były aktualizowane przez długi czas dni lub więcej w przypadku **krytycznego** i 3 dni w przypadk **ostrzeżenia**). Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsNotUpdated`.
`lastServerUpdateTime`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.2.3	Ostatni raz, kiedy antywirusowe bazy danych zostały zaktualizowane na Serwerze administracyjnym.
`hostsNotUpdated`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.2.4	Liczba urządzeń zawierających antywirusowe bazy danych, które nie są zaktualizowane.
`protectionStatus`	`INTEGER { ok(0), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.3.1	Stan ochrony w czasie rzeczywistym. Jeden z następujących: • **Ostrzeżenie**. Jeden z następujących:

			Wykryto naruszenie zabezpieczeń na urządzeniu należącym do grupy Serwer administracyjnego. Błędy szyfrowania spowodowały, że niektóre urządzenia zmieniły stan ochrony. Pełne skanowanie nie było wykonywane przez długi cza • **Krytyczne**. Ochrona antywirusowa nie działa na niektórych urządzeniach w grupach Serwera administracyjnego. • **OK**. Żadne z powyższych.
`antivirusNotRunning`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.1	Ta przyczyna wskazuje, że na niektórych urządzeniach nie działa aplikacja zabezpieczająca. Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsAntivirusNotRunning`
`realtimeNotRunning`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.2	Ta przyczyna wskazuje, że na niektórych urządzeniach nie działa ochrona w czasie rzeczywistym. Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsRealtimeNotRunning`.
`notCuredFound`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.4	Ta przyczyna wskazuje, że istnieją urządzenia zawierające niewyleczone obiekty. Liczbę tych urządzeń można uzyskać z pośrednictwem `hostsNotCuredObject`.
`tooManyThreats`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.5	Ta przyczyna wskazuje, że na niektórych urządzeniach znaleziono zagrożenia. Liczbę tych urządzeń można uzyskać z pośrednictwem `hostsTooManyThreats`.
`virusOutbreak`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.6	Ta przyczyna wskazuje stan epidemii wirusów w systemie. Wartość wynosi 1, jeśli pewna liczba wirusów została znaleziona w określonym czasie 0 w przeciwnym wypadku. Liczba wirusów i ilość czasu są określane na Serwerze administracyjnym przy użyciu ustawień `Virus attack`.
`hostsAntivirusNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.3	Liczba urządzeń z

			niedziałającymi aplikacjami zabezpieczającymi.
`hostsRealtimeNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.4	Liczba urządzeń z niedziałającą ochroną w czasie rzeczywistym
`hostsRealtimeLevelChanged`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.5	Liczba urządzeń z niedopuszczalnym poziomem ochrony w czasie rzeczywistym
`hostsNotCuredObject`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.6	Liczba urządzeń zawierających niewyleczone obiekty.
`hostsTooManyThreats`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.7	Liczba urządzeń zawierających zagrożenia.
`fullscanStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.4.1	Stan pełnego skanowania antywirusowego. Jeden z następujących: • **Informacja**. Od momentu instalacji aplikacji minęło mn niż 7 dni. • **Ostrzeżenie**. Pełne skanowanie antywirusowe n było wykonywane od ponad dni od momentu instalacji aplikacji. • **Krytyczne**. Pełne skanowan antywirusowe nie było wykonywane od ponad 14 d od momentu instalacji aplikacji. • **OK**. Żadne z powyższych.
`notScannedLately`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.4.2.1	Ta przyczyna wskazuje, że niektóre urządzenia nie były skanowane przez określony cza Liczbę tych urządzeń można uzyskać za pośrednictwem `hostsNotScannedLately`. Ilo czas jest określona w wartości `fullScanStatus`.
`hostsNotScannedLately`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.4.3	Liczba urządzeń, które nie były skanowane przez określony cza Ilość czas jest określona w wartości `fullScanStatus`.
`logicalNetworkStatus`	`INTEGER { ok(0), warning(1), critical(2) }`	.1.3.6.1.4.1.23668.1093.1.5.1	Stan sieci logicznej Serwera administracyjnego. Jeden z następujących: • **Ostrzeżenie**. Jeśli istnieją urządzenia ze stanem ostrzeżenia, do których nie można uzyskać dostępu, lub jeśli istnieją urządzenia, któr

			nie należą do żadnej grupy Serwera administracyjnego. • **Krytyczne**. Jeśli istnieją urządzenia, nad którymi kontrola została utracona przez Serwer administracyjr lub jeśli istnieją urządzenia o stanie krytycznym, do których nie można uzyskać dostępu. • **OK**. Żadne z powyższych.
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Ta przyczyna wskazuje, że niektóre urządzenia nie były połączone z Serwerem administracyjnym przez długi czas (7 lub więcej dni w przypadku urządzenia o stanie **Ostrzeżenie** i 4 dni w przypadk urządzenia o stanie **Krytyczne**) Liczbę tych urządzeń można uzyskać za pośrednictwem hostsNotConnectedLongTim
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Ta przyczyna wskazuje, że istnieją urządzenia, nad którymi kontrola została utracona przez Serwer administracyjny. Liczbę tych urządzeń można uzyskać z pośrednictwem hostsControlLost.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Liczba urządzeń znalezionych przez Serwer administracyjny, które nie należą do żadnej grup Serwera administracyjnego.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Liczba grup na Serwerze administracyjnym.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Liczba urządzeń, które nie były połączone z Serwerem administracyjnym od dłuższego czasu. Okres uważany za długi jest określony w wartości notConnectedLongTime.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Liczba urządzeń, które nie są kontrolowane przez Serwer administracyjny.
eventsStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.6.1	Status podsystemu zdarzeń. Jeden z następujących: • **Ostrzeżenie**. Jeden z następujących:

			Urządzenia grupy Serwera administracyjnego nie wyszukiwały aktualizacji systemu Windows przez dłu czas. Istnieją urządzenia z problemami ze stanem. • **Krytyczne**. Jeden z następujących: Istnieje zdarzenie o ważnośc „Krytyczne" na co najmniej jednym urządzeniu. Istnieje zdarzenie o ważnośc „Błąd" na co najmniej jednym urządzeniu. Istnieje zdarzenie zadania zakończonego niepomyślnie na co najmniej jednym urządzeniu. Urządzenia grupy Serwera administracyjnego nie wyszukiwały aktualizacji systemu Windows przez dłu czas. Istnieją urządzenia z problemami ze stanem. • **OK**. Żadne z powyższych.
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	Przyczyna, dla której stan `eventsStatus` wskazuje, że na Serwerze administracyjnym istnieją zdarzenia krytyczne. Liczbę tych zdarzeń można uzyskać, korzystając z funkcji `criticalEventsCount`. Wartość jest równa 1, jeśli na dowolnym urządzeniu występuj co najmniej jedno zdarzenie krytyczne, i 0 w innym przypadku.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Liczba zdarzeń krytycznych na Serwerze administracyjnym.

Rozwiązywanie problemów

W tej sekcji przedstawiono rozwiązania kilku typowych problemów, które mogą wystąpić podczas korzystania z usługi SNMP.

Aplikacja firmy trzeciej nie może połączyć się z usługą SNMP

Upewnij się, że obsługa protokołu SNMP jest zainstalowana w systemie Windows. Obsługa protokołu SNMP jest domyślnie wyłączona.

Aby włączyć obsługę protokołu SNMP w systemie Windows 10:

1. Przejdź do **Panelu sterowania**.
2. Otwórz menu **Dodaj lub usuń programy**.
3. Kliknij opcję **Włącz lub wyłącz funkcje systemu Windows**.
4. Na liście funkcji systemu Windows przejdź do funkcji SNMP, a następnie kliknij przycisk **OK**.
5. Przejdź do **Panel sterowania → Narzędzia administracyjne → Usługi**.
6. Wybierz usługę SNMP i uruchom ją.
7. Sprawdź, czy nasłuchiwanie działa, testując je za pomocą polecenia `netstat` w przypadku standardowego portu UPD.

Obsługa protokołu SNMP została włączona w systemie Windows 10.

Usługa SNMP działa, ale aplikacja firmy trzeciej nie może pobrać żadnych wartości

Zezwól na śledzenie agenta SNMP i upewnij się, że został utworzony niepusty plik. Oznacza to, że agent SNMP jest prawidłowo zarejestrowany i działa. Następnie zezwól na połączenia z usługi SNMP w ustawieniach usługi pobocznej. Jeśli usługa poboczna działa na tym samym hoście co agent SNMP, lista adresów IP powinna zawierać albo adres IP tego hosta, albo `loopback 127.0.0.1`.

Usługa SNMP, która komunikuje się z agentami, powinna działać w systemie Windows. Możesz określić ścieżki do agentów SNMP w rejestrze systemu Windows za pomocą programu regedit.

- Windows 10:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Windows Vista i Windows Server 2008:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

Za pomocą programu regedit możesz również zezwolić na śledzenie agentów SNMP.

- W systemach 32-bitowych:
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- W systemach 64-bitowych:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004
  "TraceDir"="C:\\"

Wartości nie pasują do stanów Konsoli administracyjnej

Aby zmniejszyć obciążenie na Serwerze administracyjnym, dla agenta SNMP zaimplementowano buforowanie wartości. Opóźnienie między aktualizacją pamięci podręcznej a zmianami wartości na Serwerze administracyjnym może powodować niezgodności między wartościami zwracanymi przez agenta SNMP i rzeczywistymi. Podczas pracy z aplikacjami firm trzecich należy wziąć pod uwagę to możliwe opóźnienie.

Praca w środowisku chmury

Ta sekcja zawiera informacje o zdalnej instalacji i konserwacji Kaspersky Security Center w środowiskach chmury, takich jak Amazon Web Services, Microsoft Azure lub Google Cloud.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Informacje o pracy w środowisku chmury

Kaspersky Security Center 14.2 pracuje nie tylko z urządzeniami lokalnymi, ale także oferuje specjalne funkcje do pracy w środowisku chmury. Kaspersky Security Center działa z następującymi maszynami wirtualnymi:

- Instancje Amazon EC2 (zwane dalej również *instancjami*). Instancja Amazon EC2 to maszyna wirtualna, która jest tworzona w oparciu o platformę Amazon Web Services (AWS). Kaspersky Security Center używa AWS *API* (Interfejs programowania aplikacji).
- Maszyny wirtualne Microsoft Azure. Kaspersky Security Center używa Azure API.
- Instancje maszyn wirtualnych Google Cloud. Kaspersky Security Center używa Google API.

Możesz zainstalować Kaspersky Security Center na instancji lub maszynie wirtualnej w celu zarządzania ochroną urządzeń w środowisku chmury i używać specjalnych funkcji Kaspersky Security Center do pracy w środowisku chmury. Te funkcje obejmują:

- Wykorzystanie narzędzi API do przeszukiwania urządzeń w środowisku chmury
- Wykorzystanie narzędzi API do zainstalowania Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w środowisku chmury
- Wyszukiwanie urządzeń w oparciu o ich przynależność do określonego segmentu chmury

Możesz również użyć instancji lub maszyny wirtualnej, na której jest zainstalowany Serwer administracyjny Kaspersky Security Center, aby chronić urządzenia lokalne (na przykład, jeśli serwer chmury okazuje się być łatwiejszy w obsłudze i utrzymaniu niż fizyczny). W takim przypadku możesz pracować z Serwerem administracyjnym tak samo, jak gdyby Serwer administracyjny był zainstalowany na urządzeniu lokalnym.

W programie Kaspersky Security Center, który został zainstalowany z płatnego obrazu Amazon Machine Image (AMI) (w AWS) lub z opcji Usage-based monthly billed SKU (w Azure), Zarządzanie poprawkami i lukami (w tym integracja z systemami SIEM) jest automatycznie aktywowane; Zarządzanie urządzeniami mobilnymi nie może zostać aktywowane.

Serwer administracyjny jest instalowany wraz z Konsolą administracyjną. Kaspersky Security for Windows Server jest także instalowany automatycznie na urządzeniu, na którym jest zainstalowany Serwer administracyjny.

Możesz skonfigurować Kaspersky Security Center za pomocą Kreatora konfiguracji środowiska chmury z uwzględnieniem specyfiki pracy w środowisku chmury.

Scenariusz: Wdrażanie ochrony dla środowiska chmury

Ta sekcja opisuje wdrażanie Kaspersky Security Center do pracy w środowiskach chmury, takich jak Amazon Web Services, Microsoft Azure i Google Cloud.

Po zakończeniu scenariusza wdrażania, elementy Serwer administracyjny Kaspersky Security Center i Konsola administracyjna zostaną uruchomione i skonfigurowane z parametrami domyślnymi. Ochrona antywirusowa zarządzana przez Kaspersky Security Center zostanie wdrożona na wybranych instancjach Amazon EC2 lub maszynach wirtualnych Microsoft Azure. Możesz dopasować konfigurację Kaspersky Security Center, utworzyć złożoną strukturę grup administracyjnych oraz utworzyć różne zasady i zadania dla grup.

Wdrożenie Kaspersky Security Center w środowisku chmury obejmuje następujące kroki:

1. Prace przygotowawcze
2. Wdrażanie Serwera administracyjnego
3. Instalowanie aplikacji antywirusowych firmy Kaspersky na urządzeniach wirtualnych, które mają być chronione
4. Konfigurowanie ustawień pobierania uaktualnień
5. Konfigurowanie ustawień zarządzania raportami dotyczącymi stanu ochrony urządzeń

Kreator konfiguracji środowiska chmury jest przeznaczony do przeprowadzania wstępnej konfiguracji. Jest uruchamiany automatycznie pierwszy raz po wdrożeniu Kaspersky Security Center z gotowego do użycia obrazu. Możesz ręcznie uruchomić kreator w dowolnym momencie. Dodatkowo możesz ręcznie wykonać wszystkie działania, które realizuje.

Zalecane jest przeznaczenie przynajmniej jednej godziny na zainstalowanie Serwera administracyjnego Kaspersky Security Center w środowisku chmury oraz przynajmniej jednego dnia roboczego na wdrożenie ochrony w środowisku chmury.

Wdrożenie Kaspersky Security Center w środowisku chmury odbywa się w krokach:

1. **Planowanie konfiguracji segmentów chmury**

   Sprawdzenie, jak Kaspersky Security Center działa w środowisku chmury. Rozplanuj, gdzie zostanie zainstalowany Serwer administracyjny: (wewnątrz lub poza środowiskiem chmury); określ także, ile segmentów chmury chcesz chronić. Jeśli planujesz zainstalować Serwer administracyjny poza środowiskiem chmury lub planujesz chronić więcej niż 5 000 urządzeń, konieczne będzie ręczne zainstalowanie Serwera administracyjnego.

   Aby pracować z Google Cloud, możesz zainstalować Serwer administracyjny tylko ręcznie.

2. **Rozplanowywanie zasobów**

   Upewnij się, że posiadasz wszystko, co jest niezbędne do wdrożenia ochrony.

3. **Subskrypcja na Kaspersky Security Center w postaci gotowego do użycia obrazu**

   Wybierz jeden z gotowych do użycia obrazów AMI w AWS Marketplace lub wybierz Usage-based monthly billed SKU w Azure Marketplace, zapłać za niego zgodnie z regułami rynku, jeśli to konieczne (lub skorzystaj z modelu BYOL) i użyj obrazu do wdrożenia instancji Amazon EC2 / maszyny wirtualnej Microsoft Azure z zainstalowanym Kaspersky Security Center.

Ten krok jest niezbędny tylko wtedy, gdy planujesz zainstalować Serwer administracyjny na instancji / maszynie wirtualnej w obrębie środowiska chmury i planujesz także wdrożenie ochrony dla ponad 5000 urządzeń. W innych sytuacjach wykonanie czynności z tego kroku nie jest konieczne, a zamiast niego konieczne jest ręczne zainstalowanie Serwera administracyjnego, Konsoli administracyjnej i DBMS.

Ten krok jest niedostępny dla Google Cloud.

4. **Określanie lokalizacji DBMS**

   Określ lokalizację Twojego systemu DBMS.

   Jeśli planujesz użyć bazy danych spoza środowiska chmury, upewnij się, że posiadasz działającą bazę danych.

   Jeśli planujesz korzystać z Amazon Relational Database Service (RDS), utwórz bazę danych z RDS w środowisku chmury AWS.

   Jeśli planujesz używać Microsoft Azure SQL DBMS, utwórz bazę danych za pomocą usługi Azure Database w środowisku chmury Microsoft Azure.

   Jeśli planujesz używać Google MySQL, utwórz bazę danych w Google Cloud (szczegóły można znaleźć na stronie https://cloud.google.com/sql/docs/mysql).

5. **Ręczne instalowanie Serwera administracyjnego i Konsoli administracyjnej (opartej na konsoli Microsoft Management Console i/lub konsoli internetowej) na wybranych urządzeniach**

   Zainstaluj Serwer administracyjny, Konsolę administracyjną i system DBMS na wybranych urządzeniach zgodnie z zaleceniami dla głównego scenariusza instalacji Kaspersky Security Center.

   Ten krok jest niezbędny, gdy planujesz umieścić Serwer administracyjny poza środowiskiem chmury lub planujesz wdrożenie ochrony dla ponad 5 000 urządzeń. Następnie upewnij się, że Twój Serwer administracyjny spełnia wymagania sprzętowe. W innych sytuacjach wykonanie czynności z tego kroku nie jest konieczne, a subskrypcja na Kaspersky Security Center w postaci gotowego do użycia obrazu w AWS Marketplace, Azure Marketplace lub Google Cloud jest wystarczająca.

6. **Zapewnianie, że Serwer administracyjny posiada uprawnienia do pracy z interfejsami API chmury**

   W AWS przejdź do konsoli zarządzania AWS i utwórz rolę IAM lub konto użytkownika IAM. Utworzona rola IAM (lub konto użytkownika IAM) umożliwi Kaspersky Security Center pracę z segmentami chmury AWS API: Poll oraz wdrożenie ochrony.

   W Azure utwórz subskrypcję oraz ID aplikacji z hasłem. Kaspersky Security Center używa tych danych uwierzytelniających do pracy z segmentami chmury Azure API: Poll i wdrożenia ochrony.

   W Google Cloud zarejestruj projekt, uzyskaj ID projektu i klucz prywatny. Kaspersky Security Center używa tych danych uwierzytelniających do przeszukiwania segmentów chmury przy użyciu Google API.

7. **Tworzenie roli IAM dla chronionych instancji (tylko dla AWS)**

   W konsoli zarządzania AWS utwórz rolę IAM, która definiuje zestaw uprawnień do wykonywania żądań wysyłanych do AWS. Ta nowo utworzona rola będzie później przypisywana do nowych instancji. Rola IAM jest wymagana do użycia Kaspersky Security Center do zainstalowania aplikacji na instancjach.

8. **Przygotowywanie bazy danych przy użyciu usługi Amazon Relational Database Service lub Microsoft Azure SQL**

   Jeśli planujesz użyć Amazon Relational Database Service (RDS), utwórz instancję bazy danych Amazon RDS i komorę S3, gdzie przechowywana będzie kopia zapasowa bazy danych. Możesz pominąć ten krok, jeśli chcesz mieć bazę danych na tej samej instancji EC2, na której jest zainstalowany Serwer administracyjny, lub jeśli chcesz, aby Twoja baza danych znajdowała się w innym miejscu.

   Jeśli panujesz użyć Microsoft Azure SQL, utwórz konto magazynu i bazę danych w Microsoft Azure.

   Jeśli planujesz używać Google MySQL, skonfiguruj bazę danych w Google Cloud (szczegóły można znaleźć na stronie https://cloud.google.com/sql/docs/mysql).

9. **Licencjonowanie Kaspersky Security Center do pracy w środowisku chmury**

Upewnij się, że posiadasz licencjonowaną wersję Kaspersky Security Center, aby pracować w środowisku chmury, i dostarcz kod aktywacyjny lub plik klucza, aby aplikacja mogła dodać go do magazynu licencji. Ten etap można zakończyć podczas konfiguracji środowiska chmury.

Ten krok jest wymagany, jeśli korzystasz z programu Kaspersky Security Center zainstalowanego z bezpłatnego, gotowego do użycia obrazu AMI na podstawie modelu BYOL lub jeśli ręcznie instalujesz Kaspersky Security Center bez użycia obrazów AMI. W każdym z tych przypadków będziesz potrzebował licencji dla Kaspersky Security for Virtualization lub licencji dla Kaspersky Hybrid Cloud Security, aby aktywować Kaspersky Security Center.

Jeśli używasz Kaspersky Security Center zainstalowanego z gotowego do użycia obrazu, ten etap nie jest konieczny, a odpowiednie okno Kreatora konfiguracji środowiska chmury nie jest wyświetlane.

10. **Autoryzacja w środowisku chmury**

    Dostarcz Kaspersky Security Center swoje dane uwierzytelniające AWS, Azure lub Google Cloud, aby Kaspersky Security Center mógł działać z potrzebnymi uprawnieniami. Ten etap można zakończyć podczas autoryzacji w środowisku chmury.

11. **Przeszukiwanie segmentu chmury, aby Serwer administracyjny mógł uzyskać informacje o urządzeniach w segmencie chmury**

    Uruchom przeszukiwanie segmentu chmury. W środowisku AWS Kaspersky Security Center uzyska adresy i nazwy wszystkich instancji, do których dostęp można uzyskać w oparciu o uprawnienia roli IAM lub użytkownika IAM. W środowisku Microsoft Azure Kaspersky Security Center uzyska adresy i nazwy wszystkich maszyn wirtualnych, do których dostęp można uzyskać w oparciu o uprawnienia roli Czytelnik.

    Następnie możesz użyć Kaspersky Security Center do zainstalowania aplikacji firmy Kaspersky i oprogramowania innych producentów na wykrytych instancjach lub maszynach wirtualnych.

    Kaspersky Security Center regularnie wykonuje przeszukiwanie, co oznacza, że nowe instancje lub maszyny wirtualne są wykrywane automatycznie.

12. **Przyłączanie wszystkich urządzeń sieciowych do grupy administracyjnej Chmura**

    Przenieś wszystkie wykryte instancje /maszyny wirtualne do grupy administracyjnej **Zarządzane urządzenia\Chmura**, aby mogły stać się dostępne do scentralizowanego zarządzania. Jeśli chcesz przydzielić urządzenia do podgrup, na przykład, według zainstalowanego na nich systemu operacyjnego, w grupie **Zarządzane urządzenia\Chmura** możesz utworzyć kilka grup administracyjnych. Możesz włączyć automatyczne przenoszenie wszystkich urządzeń, które zostaną wykryte podczas rutynowego przeszukiwania, do grupy **Zarządzane urządzenia\Chmura**.

13. **Używanie Agenta sieciowego do podłączania urządzeń w sieci do Serwera administracyjnego**

    Zainstaluj Agenta sieciowego na urządzeniach w środowisku chmury. Agent sieciowy jest komponentem Kaspersky Security Center, który zapewnia komunikację pomiędzy urządzeniami a Serwerem administracyjnym. Domyślnie ustawienia Agenta sieciowego są konfigurowane automatycznie.

    Możesz zainstalować Agenta sieciowego na każdym urządzeniu lokalnie. Możesz także zdalnie zainstalować Agenta sieciowego na urządzeniach przy użyciu Kaspersky Security Center. Lub możesz pominąć ten krok i zainstalować Agenta sieciowego wraz z najnowszymi wersjami aplikacji zabezpieczających.

14. **Instalowanie najnowszych wersji aplikacji zabezpieczających na urządzeniach w sieci**

    Wybierz urządzenia, na których chcesz zainstalować aplikacje zabezpieczające, a następnie zainstaluj najnowsze wersje aplikacji zabezpieczających na tych urządzeniach. Instalację można przeprowadzić zdalnie przy użyciu Kaspersky Security Center na Serwerze administracyjnym lub lokalnie.

    Konieczne może być ręczne utworzenie pakietów instalacyjnych dla tych programów.

    Kaspersky Endpoint Security for Linux jest przeznaczony dla instancji i maszyn wirtualnych działających pod kontrolą systemu Linux.

    Kaspersky Security for Windows Server jest przeznaczony dla instancji i maszyn wirtualnych działających pod kontrolą systemu Windows.

15. **Konfigurowanie ustawień aktualizacji**

Zadanie **Wyszukiwanie luk i wymaganych aktualizacji** jest tworzone automatycznie po uruchomieniu konfiguracji środowiska chmury. Możesz także ręcznie utworzyć zadanie. To zadanie automatycznie wyszukuje i pobiera wymagane aktualizacje aplikacji dla instalacji na urządzeniach w sieci przy użyciu narzędzi Kaspersky Security Center.

Po zakończeniu konfiguracji środowiska chmury zaleca się wykonanie następującego etapu:

1. **Konfigurowanie zarządzania raportami**

   Możesz przejrzeć raporty na zakładce **Monitorowanie** w obszarze roboczym węzła **Serwer administracyjny** i/lub otrzymać raporty za pośrednictwem poczty elektronicznej. Raporty możesz otrzymać także za pośrednictwem poczty elektronicznej. Raporty na zakładce **Monitorowanie** są dostępne domyślnie. Aby skonfigurować otrzymywanie raportów za pośrednictwem poczty elektronicznej, określ adresy e-mail, na które powinny przychodzić raporty, a następnie skonfiguruj format raportów.

Wyniki

Po zakończeniu scenariusza możesz upewnić się, że wstępna konfiguracja zakończyła się pomyślnie:

- Możesz nawiązać połączenie z Serwerem administracyjnym poprzez Konsolę administracyjną lub Kaspersky Security Center Web Console.
- Najnowsze wersje aplikacji zabezpieczających Kaspersky są zainstalowane i uruchomione na zarządzanych urządzeniach.
- Kaspersky Security Center utworzył domyślne zasady i zadania dla wszystkich zarządzanych urządzeń.

Wymagania wstępne wdrożenia Kaspersky Security Center w środowisku chmury

Przed rozpoczęciem wdrożenia Kaspersky Security Center w środowisku chmury Amazon Web Services lub Microsoft Azure, upewnij się, że posiadasz:

- Dostęp do internetu
- Jedno z następujących kont:
  - Konto Amazon Web Services (do pracy z AWS)
  - Konto Microsoft (do pracy z Azure)
  - Konto Google (do pracy z Google Cloud)
- Jeden z następujących:
  - Licencję dla Kaspersky Security for Virtualization
  - Licencję dla Kaspersky Hybrid Cloud Security
  - Fundusze na zakup takiej licencji (Kaspersky Security for Virtualization lub Kaspersky Hybrid Cloud Security)
  - Fundusze na zakup gotowego do użycia obrazu w Azure Marketplace

- Podręczniki dla najnowszych wersji Kaspersky Endpoint Security for Linux i Kaspersky Security for Windows Server

Wymagania sprzętowe dla Serwera administracyjnego w środowisku chmury

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

Opcje licencjonowania w środowisku chmury

Praca w środowisku chmury jest poza podstawową funkcjonalnością Kaspersky Security Center, więc wymaga to specjalnej licencji.

Do pracy w środowisku chmury dostępne są dwie opcje licencjonowania Kaspersky Security Center:

- Paid AMI (w Amazon Web Services) / Usage-based monthly billed SKU (w Microsoft Azure).

  Przyznaje to licencję dla Kaspersky Security Center, a także licencje dla Kaspersky Endpoint Security for Linux i Kaspersky Security for Windows Server. Musisz zapłacić zgodnie z regułami środowiska chmury, którego używasz.

  Ten model pozwala na posiadanie nie więcej niż 200 urządzeń klienckich dla jednego Serwera administracyjnego.

- Bezpłatny, gotowy do użycia obraz za pomocą własnościowej licencji, zgodnie z modelem Bring Your Own License (BYOL).

  W przypadku licencjonowania Kaspersky Security Center w AWS lub Azure, należy posiadać licencję dla jednej z następujących aplikacji:

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  Model BYOL pozwala na posiadanie do 100 000 urządzeń klienckich dla jednego Serwera administracyjnego. Ten model umożliwia także zarządzanie urządzeniami spoza środowiska chmury AWS, Azure lub Google.

  Model BYOL można wybrać w jednym z następujących przypadków:

  - Jeśli masz już ważną licencję dla Kaspersky Security for Virtualization.
  - Jeśli masz już ważną licencję dla Kaspersky Hybrid Cloud Security.
  - Jeśli chcesz zakupić licencję bezpośrednio przed zdalną instalacją Kaspersky Security Center.

  Na etapie wstępnej konfiguracji Kaspersky Security Center wyświetli okno z prośbą o podanie kodu aktywacyjnego lub pliku klucza.

  Jeśli wybierzesz BYOL, nie musisz płacić za Kaspersky Security Center za pośrednictwem Azure Marketplace lub AWS Marketplace.

W obu przypadkach automatycznie aktywowane jest Zarządzanie lukami i poprawkami, a Zarządzanie urządzeniami mobilnymi nie może zostać aktywowane.

Podczas próby aktywacji funkcji Obsługa środowiska chmury przy użyciu licencji dla Kaspersky Hybrid Cloud Security może wystąpić błąd.

Po wykupieniu subskrypcji na Kaspersky Security Center, otrzymujesz instancję Amazon Elastic Compute Cloud (Amazon EC2) lub maszynę wirtualną Microsoft Azure z Serwerem administracyjnym Kaspersky Security Center. Pakiety instalacyjne dla Kaspersky Security for Windows Server i Kaspersky Endpoint Security for Linux są dostępne na Serwerze administracyjnym. Możesz zainstalować te aplikacje na urządzeniach w środowisku chmury. Nie musisz licencjonować tych aplikacji.

Jeśli zarządzane urządzenie nie jest widoczne dla Serwera administracyjnego przez ponad tydzień, aplikacja (Kaspersky Security for Windows Server lub Kaspersky Endpoint Security for Linux) na urządzeniu przełączy się do trybu ograniczonej funkcjonalności. Aby aktywować aplikację ponownie, urządzenie, na której zainstalowana jest ta aplikacja, musi ponownie stać się widoczne dla Serwera administracyjnego.

Opcje bazy danych do pracy w środowisku chmury

Musisz mieć bazę danych, aby pracować z Kaspersky Security Center. Podczas instalowania Kaspersky Security Center w AWS, w Microsoft Azure lub Google Cloud masz trzy opcje:

- Utwórz lokalną bazę danych na tym samym urządzeniu co Serwer administracyjny. Kaspersky Security Center jest dostarczany z bazą danych SQL Server Express, która może obsługiwać do 5 000 zarządzanych urządzeń. Wybierz tę opcję, jeśli SQL Server Express Edition jest wystarczający dla Twoich potrzeb.

- Utwórz bazę danych z Relational Database Service (RDS) w środowisku chmury AWS lub z usługi Azure Database w środowisku chmury Microsoft Azure. Wybierz tę opcję, jeśli chcesz system DBMS inny niż SQL Express. Twoje dane zostaną przesłane wewnątrz środowiska chmury, gdzie pozostaną, i nie będziesz ponosił dodatkowych wydatków. Jeśli już pracujesz z Kaspersky Security Center na urządzeniach lokalnych i posiadasz pewne dane w swojej bazie danych, możesz przenieść swoje dane do nowej bazy danych.

  Do pracy na platformie Google Cloud Platform możesz użyć tylko Cloud SQL for MySQL.

- Użyj istniejącego serwera bazy danych. Wybierz tę opcję, jeśli już posiadasz serwer bazy danych i chcesz go używać dla Kaspersky Security Center. Jeśli ten serwer znajduje się poza środowiskiem chmury, Twoje dane zostaną przesłane przez internet, co może generować dodatkowe koszty.

Procedura wdrażania Kaspersky Security Center w środowisku chmury posiada specjalny krok tworzenia (wybierania) bazy danych.

Praca w środowisku chmury Amazon Web Services

Ta sekcja opisuje sposób przygotowania pracy z Kaspersky Security Center w Amazon Web Services.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Informacje o pracy w środowisku chmury Amazon Web Services

Kaspersky Security Center można kupić w sklepie AWS Marketplace w postaci Amazon Machine Image (AMI), która jest gotowym do użycia obrazem wstępnie skonfigurowanej maszyny wirtualnej. Możesz wykupić subskrypcję na płatny obraz AMI lub BYOL AMI i na podstawie tego obrazu utworzyć instancję Amazon EC2 z zainstalowanym Serwerem administracyjnym Kaspersky Security Center.

Aby pracować z platformą AWS, a w szczególności kupić aplikacje w sklepie AWS Marketplace i tworzyć instancje, będziesz potrzebował konta Amazon Web Services. Możesz utworzyć darmowe konto na stronie https://aws.amazon.com. Możesz także użyć istniejącego konta Amazon.

Jeśli wykupiłeś subskrypcję na obraz AMI, dostępny w sklepie AWS Marketplace, otrzymasz instancję z gotowym do użycia Kaspersky Security Center. Nie trzeba instalować aplikacji samodzielnie. W takim przypadku Serwer administracyjny Kaspersky Security Center jest instalowany na instancji bez Twojego udziału. Po instalacji, możesz uruchomić Konsolę administracyjną i połączyć się z Serwerem administracyjnym, aby rozpocząć pracę z Kaspersky Security Center.

W celu uzyskania bardziej szczegółowych informacji na temat obrazu AMI oraz działania AWS Marketplace, odwiedź stronę pomocy AWS Marketplace. Aby uzyskać więcej informacji na temat pracy z platformą AWS, używania instancji oraz powiązanych pojęć, zapoznaj się z dokumentacją Amazon Web Services.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie roli IAM i kont użytkowników IAM dla instancji Amazon EC2

Ta sekcja opisuje działania, jakie muszą zostać wykonane w celu zapewnienia poprawnego działania Serwera administracyjnego. Te działania obejmują pracę z rolami AWS Identity i Access Management (IAM) i kontami użytkowników. Opisane są także działania, które muszą zostać wykonane na urządzeniach klienckich w celu zainstalowania na nich Agenta sieciowego, a następnie zainstalowania Kaspersky Security for Windows Server i Kaspersky Endpoint Security for Linux.

Zapewnianie, że Serwer administracyjny Kaspersky Security Center posiada uprawnienia do pracy z AWS

Standardy działania środowiska chmury Amazon Web Services zalecają, aby specjalna rola IAM była przypisywana do instancji Serwera administracyjnego do pracy z usługami AWS. Rola IAM to jednostka IAM, która definiuje zestaw uprawnień do wykonywania żądań wysyłanych do usług AWS. Rola IAM zapewnia uprawnienia dla przeszukiwania segmentu chmury i instalacji aplikacji na instancjach.

Po utworzeniu roli IAM i przypisaniu jej do Serwera administracyjnego, będziesz mógł wdrożyć ochronę instancji przy użyciu tej roli, bez dostarczania jakichkolwiek dodatkowych informacji do Kaspersky Security Center.

Jednakże zalecane jest, aby nie tworzyć roli IAM dla Serwera administracyjnego w następujących przypadkach:

- Urządzenia, których ochroną planujesz zarządzać, to instancje EC2 w środowisku chmury Amazon Web Services, ale Serwer administracyjny znajduje się poza tym środowiskiem.

- Planujesz zarządzać ochroną instancji nie tylko w obrębie swojego segmentu chmury, ale także w innych segmentach chmury, które zostały utworzone z poziomu innego konta w AWS. W tym przypadku będziesz potrzebował roli IAM tylko do ochrony swojego segmentu chmury. Rola IAM nie będzie potrzebna do ochrony innego segmentu chmury.

W tych przypadkach, zamiast utworzenia roli IAM będziesz musiał utworzyć *konto użytkownika IAM*, które będzie używane przez Kaspersky Security Center do pracy z usługami AWS. Przed rozpoczęciem pracy z Serwerem administracyjnym utwórz Konto użytkownika IAM z *Kluczem dostępu IAM AWS* (zwany dalej również *Klucz dostępu IAM*).

Do utworzenia roli IAM oraz konta użytkownika IAM wymagana jest konsola AWS Management Console. Aby pracować z konsolą AWS Management Console, potrzebna jest nazwa użytkownika i hasło dla konta w AWS.

Tworzenie roli IAM dla Serwera administracyjnego

Przed zainstalowaniem Serwera administracyjnego, w konsoli AWS Management Console utwórz rolę IAM z uprawnieniami wymaganymi do zainstalowania aplikacji na instancjach. Więcej informacji znajdziesz w sekcjach pomocy AWS o rolach IAM.

W celu utworzenia roli IAM dla Serwera administracyjnego:

1. Otwórz konsolę AWS Management Console i zaloguj się z poziomu konta AWS.
2. W sekcji **Role** utwórz rolę z następującymi uprawnieniami:
   - **AmazonEC2ReadOnlyAccess**, jeśli planujesz tylko uruchamiać przeszukiwanie segmentów chmury, a nie chcesz instalować aplikacji na instancjach EC2 przy użyciu AWS API.
   - **AmazonEC2ReadOnlyAccess** i **AmazonSSMFullAccess**, jeśli planujesz uruchamiać przeszukiwanie segmentów chmury i chcesz instalować aplikacje na instancjach EC2 przy użyciu AWS API. W tym przypadku konieczne będzie też przypisanie roli IAM z uprawnieniem AmazonEC2RoleforSSM do chronionych instancji EC2.

Będziesz musiał przypisać tę rolę do instancji EC2, której będziesz używał jako Serwera administracyjnego.

Nowo utworzona rola jest dostępna dla wszystkich aplikacji na Serwerze administracyjnym. Dlatego też każda aplikacja uruchomiona na Serwerze administracyjnym posiada możliwość przeszukiwania segmentów chmury lub instalowania aplikacji na instancjach EC2 w segmencie chmury.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie konta użytkownika IAM do pracy z Kaspersky Security Center

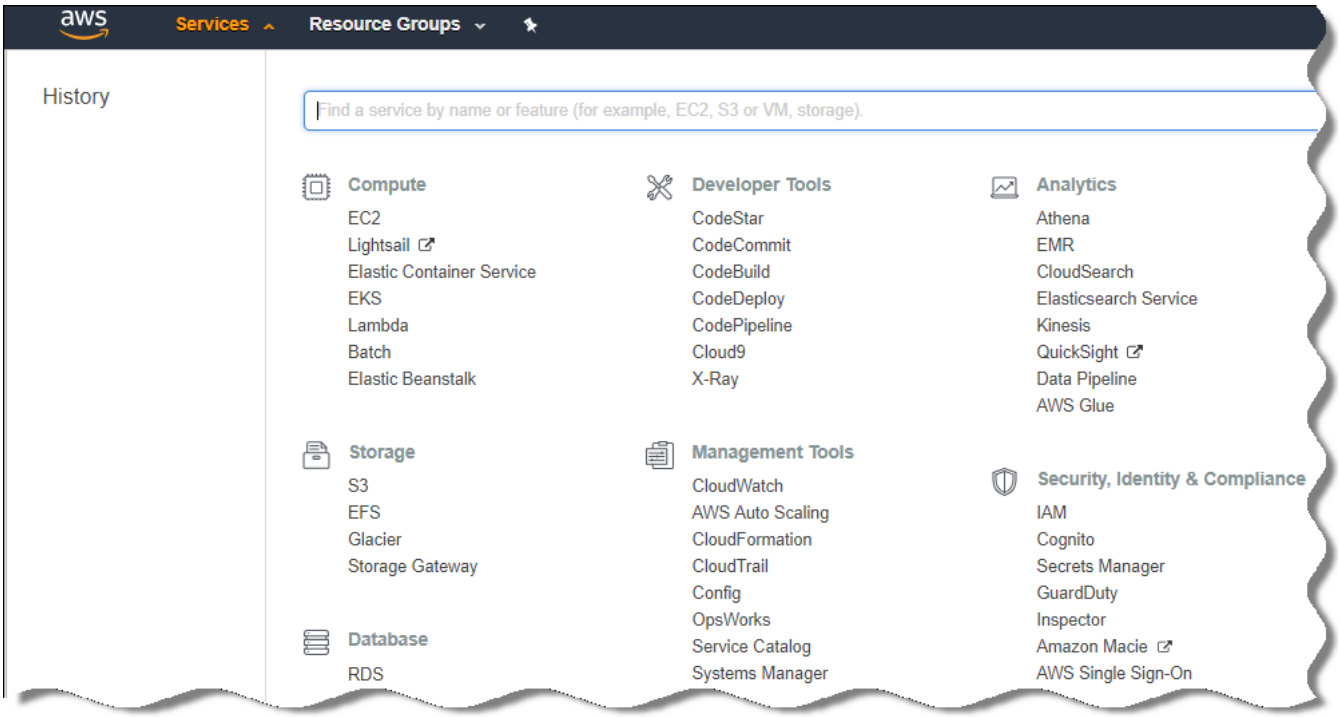
Konto użytkownika IAM jest wymagane do pracy z Kaspersky Security Center, jeśli do Serwera administracyjnego nie przypisano roli IAM z uprawnieniami do wyszukiwania urządzeń i instalacji aplikacji na instancjach. To samo konto lub inne konto jest także wymagane dla zadania tworzenia kopii zapasowej danych Serwera administracyjnego, jeśli używasz komory S3. Możesz utworzyć jedno konto użytkownika IAM ze wszystkimi niezbędnymi uprawnieniami lub możesz utworzyć dwa oddzielne konta użytkownika.

Klucz dostępu IAM, który będziesz musiał dostarczyć Kaspersky Security Center podczas wstępnej konfiguracji, jest automatycznie tworzony dla użytkownika IAM. Klucz dostępu IAM składa się z identyfikatora klucza dostępu i tajnego klucza. Więcej informacji na temat usługi IAM można znaleźć na następujących stronach referencyjnych AWS:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

W celu utworzenia konta użytkownika IAM z potrzebnymi uprawnieniami:

1. Otwórz konsolę AWS Management Console i zaloguj się z poziomu swojego konta.
2. Na liście usług AWS wybierz **IAM** (jak pokazano na poniższym rysunku).



Lista usług w konsoli AWS Management Console

Zostanie otwarte okno zawierające listę nazw użytkowników i menu, które umożliwia pracę z narzędziem.

3. Poruszaj się po obszarach konsoli związanych z kontami użytkownika i dodaj nową nazwę lub nazwy użytkownika.
4. Dla dodawanego użytkownika (użytkowników) określ następujące właściwości AWS:
   - Typ dostępu: **Programmatic Access**.
   - Granice uprawnień nie są określone.
   - Uprawnienia:
     - **ReadOnlyAccess**—jeśli planujesz tylko uruchamiać przeszukiwanie segmentów chmury, a nie chcesz instalować aplikacji na instancjach EC2 przy użyciu AWS API.
     - **ReadOnlyAccess** i **AmazonSSMFullAccess**—jeśli planujesz uruchamiać przeszukiwanie segmentów chmury i chcesz instalować aplikacje na instancjach EC2 przy użyciu AWS API. W tym przypadku konieczne będzie też przypisanie roli IAM z uprawnieniem AmazonEC2RoleforSSM do chronionych instancji EC2.

Po dodaniu uprawnień sprawdź je pod kątem prawidłowości. W przypadku omyłkowego wyboru wróć do poprzedniego okna i ponownie dokonaj wyboru.

5. Po utworzeniu konta użytkownika, zostanie wyświetlona tabela zawierająca klucz dostępu IAM nowego użytkownika IAM. Identyfikator klucza dostępu zostanie wyświetlony w kolumnie **Access Key ID**. Tajny klucz będzie wyświetlany od postacią gwiazdek w kolumnie **Tajny klucz dostępu**. Aby sprawdzić tajny klucz, kliknij **Pokaż**.

Nowo utworzone konto zostanie wyświetlone na liście kont użytkowników IAM odpowiadających Twojemu kontu w AWS.

Podczas wdrażania Kaspersky Security Center w segmencie chmury musisz określić, że korzystasz z konta użytkownika IAM, oraz dostarczyć identyfikator klucza dostępu i tajny klucz dostępu do Kaspersky Security Center.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie roli IAM dla instalacji aplikacji na instancjach Amazon EC2

Przed rozpoczęciem wdrażania ochrony na instancjach EC2 przy użyciu Kaspersky Security Center, utwórz w konsoli zarządzania AWS rolę IAM z uprawnieniami wymaganymi do instalacji aplikacji na instancjach. Więcej informacji o rolach IAM znajdziesz w sekcjach pomocy AWS.

Rola IAM jest potrzebna, aby móc ją przypisać do wszystkich instancji EC2, na których planujesz zainstalować aplikacje zabezpieczające przy użyciu Kaspersky Security Center. Jeśli nie przypiszesz do instancji roli IAM z wymaganymi uprawnieniami, instalacja aplikacji na tej instancji przy użyciu narzędzi AWS API zakończy się błędem.

Aby pracować z konsolą AWS Management Console, potrzebna jest nazwa użytkownika i hasło dla konta w AWS.

W celu utworzenia roli IAM dla instalacji aplikacji na instancjach:

1. Otwórz konsolę AWS Management Console i zaloguj się z poziomu konta AWS.
2. Z menu po lewej stronie wybierz **Roles**.
3. Kliknij przycisk **Create Role**.
4. Na liście usług, która zostanie wyświetlona, wybierz **EC2**, a następnie, na liście **Select Your Use Case** ponownie wybierz **EC2**.
5. Kliknij przycisk **Next: Permissions**.
6. Na otwartej liście zaznacz pole obok **AmazonEC2RoleforSSM**.
7. Kliknij przycisk **Next: Review**.
8. Wprowadź nazwę i opis dla roli IAM i kliknij przycisk **Create role**.

   Utworzona rola pojawi się na liście roli z wprowadzoną nazwą i opisem.

Możesz użyć nowo utworzonej roli IAM do utworzenia nowych instancji EC2, które chcesz chronić poprzez Kaspersky Security Center, a także skojarzyć ją z istniejącymi instancjami.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Praca z Amazon RDS

Ta sekcja opisuje, które akcje muszą zostać podjęte, aby przygotować bazę danych Amazon Relational Database Service (RDS) dla Kaspersky Security Center, umieścić ją w grupie opcji, utworzyć rolę IAM do pracy z bazą danych RDS, przygotować zasobnik S3 do przechowywania i przenieść istniejącą bazę danych do RDS.

Amazon RDS to usługa sieciowa, która pomaga użytkownikom AWS w skonfigurowaniu, działaniu i skalowaniu relacyjnych baz danych w środowisku chmury AWS. Jeśli chcesz, możesz użyć bazy danych Amazon RDS do pracy z Kaspersky Security Center.

Możesz pracować z następującymi bazami danych:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Tworzenie instancji Amazon RDS

Jeśli chcesz użyć Amazon RDS jako DBMS, musisz utworzyć instancję bazy danych Amazon RDS. Ta sekcja opisuje sposób wybrania SQL Express Edition; jeśli chcesz pracować z Aurora MySQL lub Standard MySQL (wersje 5.7, 8.0), powinieneś wybrać jeden z tych silników.

W celu utworzenia instancji bazy danych Amazon RDS:

1. Otwórz konsolę AWS Management Console, dostępną pod adresem https://console.aws.amazon.com, a następnie zaloguj się z poziomu swojego konta.
2. Korzystając z interfejsu AWS, utwórz bazę danych z następującymi ustawieniami:
   - Engine: Microsoft SQL Server, SQL Express Edition
   - Wersja silnika DB: SQL Server 2014 12.00.5546.0v1
   - Klasa instancji DB: db.t2.medium
   - Typ magazynu: General purpose
   - Przydzielony magazyn: minimum 50 GiB
   - Grupa bezpieczeństwa: ta sama grupa, w której znajduje się instancja EC2 z Serwerem administracyjnym Kaspersky Security Center

   Dla swojej instancji RDS utwórz identyfikator, nazwę użytkownika i hasło.

W pozostałych polach możesz zostawić domyślne ustawienia. Lub zmienić domyślne ustawienia, jeśli chcesz dostosować swoją instancję Amazon RDS. Aby uzyskać pomoc, sprawdź strony informacyjne AWS.

3. W ostatnim kroku AWS wyświetli wyniki procesu. Jeśli chcesz przejrzeć szczegóły swojej instancji Amazon RDS, kliknij **View DB instance details**. Jeśli chcesz przejść do kolejnego działania, rozpocznij tworzenie grupy opcji dla swojej instancji Amazon RDS.

Tworzenie nowej instancji Amazon RDS może potrwać kilka minut. Po utworzeniu instancji, możesz jej użyć do pracy z danymi Kaspersky Security Center.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie grupy opcji dla instancji Amazon RDS

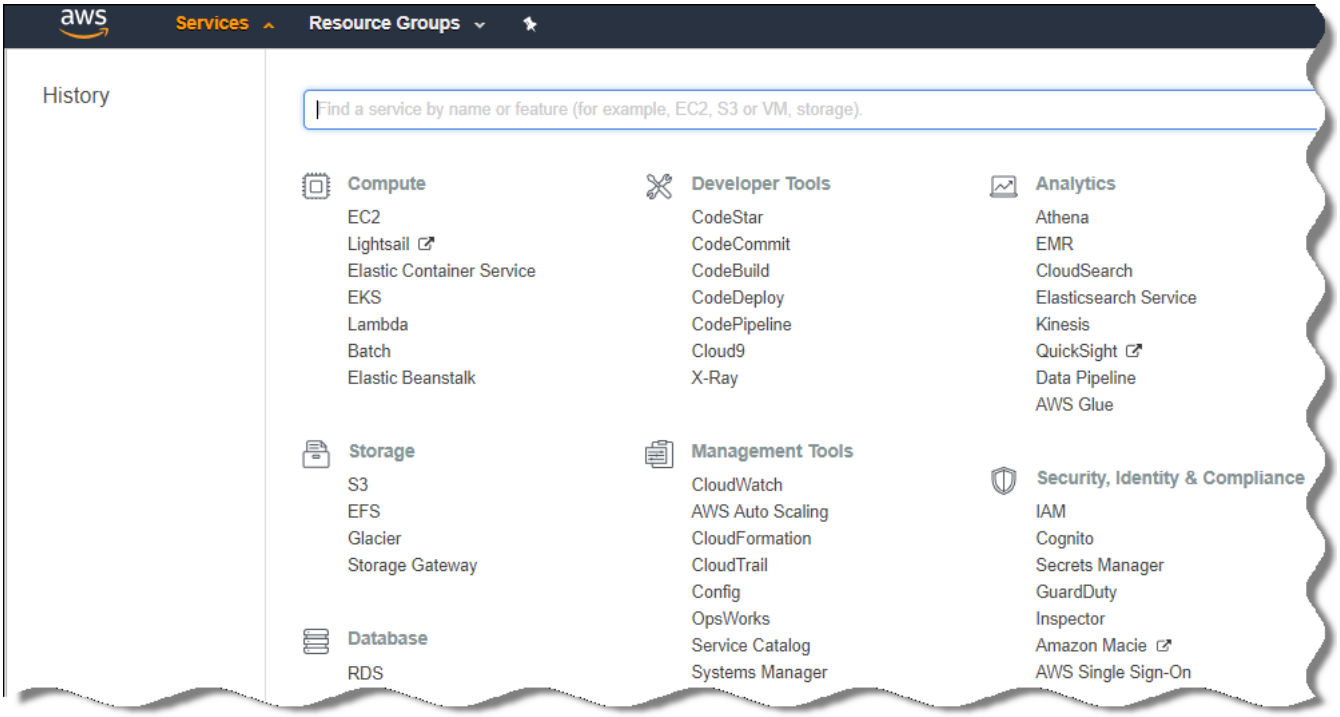
Musisz umieścić swoją instancję Amazon RDS w grupie opcji.

W celu utworzenia grupy opcji dla swojej instancji Amazon RDS:

1. Upewnij się, że jesteś w konsoli AWS Management Console (https://console.aws.amazon.com) i zalogowałeś się do niej z poziomu swojego konta.

2. W wierszu menu kliknij **Usługi**.

   Zostanie wyświetlona lista dostępnych usług (patrz rysunek poniżej).



Lista usług w konsoli AWS Management Console

3. Na liście kliknij **RDS**.

4. W lewym panelu kliknij **Grupy opcji**.

5. Kliknij przycisk **Create group**.

6. Jeśli na etapie tworzenia instancji Amazon RDS wybrałeś serwer SQL, utwórz grupę opcji z następującymi ustawieniami:

   - Engine: SQLserver-ex
   - Major engine version: 12.00

   Jeśli na etapie tworzenia instancji Amazon RDS wybrałeś inną bazę danych SQL, wybierz odpowiedni silnik.

   Grupa zostanie utworzona i będzie wyświetlana na liście grup.

Po utworzeniu grupy opcji, umieść swoją instancję Amazon RDS w tej grupie opcji.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Modyfikowanie grupy opcji

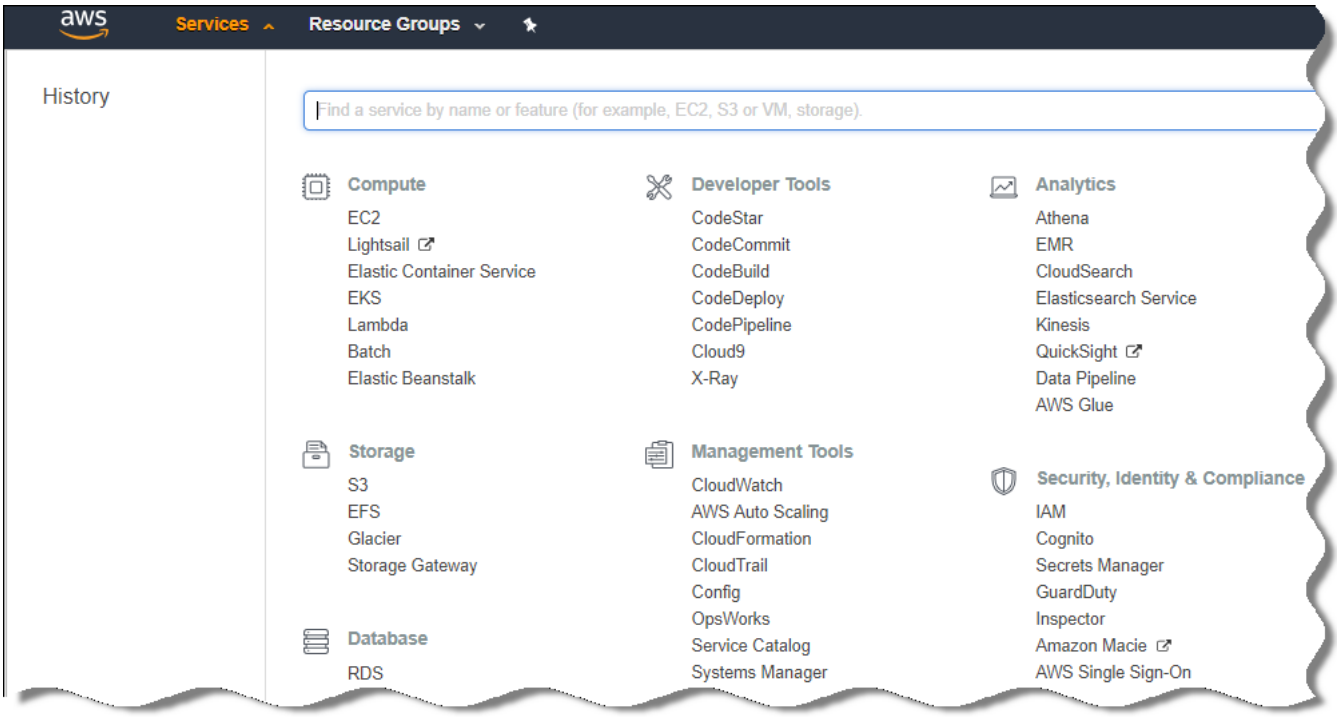
Domyślna konfiguracja grupy opcji, w której umieściłeś instancję Amazon RDS nie jest wystarczająca do pracy z bazą danych Kaspersky Security Center. Musisz dodać opcje do grupy opcji i utworzyć nową rolę IAM do pracy z bazą danych.

W celu zmodyfikowania grupy opcji i utworzenia nowej roli IAM:

1. Upewnij się, że jesteś w konsoli AWS Management Console (https://console.aws.amazon.com) i zalogowałeś się do niej z poziomu swojego konta.

2. W wierszu menu kliknij **Usługi**.

   Zostanie wyświetlona lista dostępnych usług (patrz rysunek poniżej).



Lista usług w konsoli AWS Management Console

3. Na liście wybierz RDS.

4. W lewym panelu kliknij **Grupy opcji**.

   Zostanie wyświetlona lista grup opcji.

5. Wybierz grupę opcji, w której umieściłeś swoją instancję Amazon RDS, i kliknij przycisk **Dodaj opcję**.

   Zostanie otwarte okno **Dodaj opcję**.

6. W sekcji Rola IAM wybierz opcję **Utwórz nową rolę** / **Tak** i wprowadź nazwę nowej roli IAM.

   Rola jest tworzona z domyślnym zestawem uprawnień. Następnie będziesz musiał zmienić jej uprawnienia.

7. W sekcji Komora S3 wykonaj jedną z następujących czynności:

   - Jeśli nie utworzyłeś instancji komory Amazon S3 dla kopii zapasowej danych, wybierz odnośnik **Utwórz nową komorę S3** i utwórz nową komorę S3, korzystając z interfejsu S3.
   - Jeśli już utworzyłeś instancję komory Amazon S3 dla zadania tworzenia kopii zapasowej danych Serwera administracyjnego, wybierz swoją komorę S3 z menu rozwijalnego.

8. Zakończ dodawanie opcji, klikając przycisk **Dodaj opcję** w dolnej części strony.

Zmodyfikowałeś grupę opcji i utworzyłeś nową rolę IAM do pracy z bazą danych RDS.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Modyfikowanie uprawnień dla roli IAM dla instancji bazy danych Amazon RDS

Po dodaniu opcji do grupy opcji, musisz przypisać wymagane uprawnienia do roli IAM, którą utworzyłeś do pracy z instancją bazy danych Amazon RDS.

W celu przypisania wymaganych uprawnień do roli IAM, którą utworzyłeś do pracy z instancją bazy danych Amazon RDS:

1. Upewnij się, że jesteś w konsoli AWS Management Console (https://console.aws.amazon.com) i zalogowałeś się do niej z poziomu swojego konta.

2. Na liście usług wybierz **IAM**.

   Zostanie otwarte okno zawierające listę nazw użytkowników i menu, które umożliwia pracę z narzędziem.

3. W menu wybierz **Role**.

4. Na liście ról IAM, wyświetlonych w obszarze roboczym, wybierz rolę, którą utworzyłeś podczas dodawania opcji do grupy opcji.

5. Korzystając z interfejsu AWS, usuń profil **sqlNativeBackup-<date>**.

6. Korzystając z interfejsu AWS, przyłącz profil **AmazonS3FullAccess** do roli.

Do roli IAM zostają przypisane wymagane uprawnienia do pracy z Amazon RDS.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Przygotowanie komory Amazon S3 dla bazy danych

Jeśli planujesz korzystać z bazy danych Amazon Relational Database System (Amazon RDS), musisz utworzyć instancję komory Amazon Simple Storage Service (Amazon S3), gdzie będzie przechowywana regularna kopia zapasowa bazy danych. Informacje o komorze Amazon S3 i komorze S3 znajdziesz na stronach pomocy Amazon. Więcej informacji na temat tworzenia instancji Amazon S3 znajdziesz na stronie pomocy Amazon S3.

W celu utworzenia komory Amazon S3:

1. Upewnij się, że konsola AWS Management Console jest otwarta i zalogowałeś się na swoje konto.
2. Na liście usług AWS wybierz S3.
3. Nawiguj po konsoli, aby utworzyć komorę, wykonując instrukcje kreatora.
4. Wybierz ten sam region, w którym znajduje się Serwer administracyjny (lub będzie się znajdował).
5. Jeśli kreator zakończy pracę, upewnij się, że nowa komora pojawi się na liście komór.

   Nowa komora S3 została utworzona i pojawiła się na Twojej liście komór. Musisz określić tę komorę podczas dodawania opcji do grupy opcji. Będziesz musiał także określić adres Twojej komory S3 do Kaspersky Security Center, gdy Kaspersky Security Center tworzy zadanie *Kopia zapasowa danych Serwera administracyjnego*.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Przenoszenie bazy danych do Amazon RDS

Możesz przenieść swoją bazę danych Kaspersky Security Center z urządzenia lokalnego do instancji Amazon S3, która obsługuje Amazon RDS. Aby to zrobić, potrzebujesz komory S3 dla bazy danych RDS i konta użytkownika IAM z uprawnieniem AmazonS3FullAccess dla tej komory S3.

W celu przeniesienia bazy danych:

1. Upewnij się, że utworzyłeś instancję RDS (więcej informacji znajdziesz na stronach referencyjnych Amazon RDS).
2. Na swoim fizycznym Serwerze administracyjnym (lokalnym) uruchom narzędzie Kaspersky Backup, aby utworzyć kopię zapasową danych Serwera administracyjnego.

   Musisz upewnić się, że plik nosi nazwę backup.zip.
3. Skopiuj plik backup.zip na instancję EC2, na której jest zainstalowany Serwer administracyjny.

Upewnij się, że posiadasz wystarczającą ilość miejsca na instancji EC2, na której jest zainstalowany Serwer administracyjny. W środowisku AWS możesz dodać przestrzeń dyskową do swojej instancji, aby ulokować proces migracji bazy danych.

4. Na Serwerze administracyjnym AWS uruchom ponownie narzędzie Kaspersky Backup w trybie interaktywnym.

   Zostanie uruchomiony Kreator tworzenia kopii zapasowej i przywracania.

5. W kroku **Wybierz akcję** wybierz **Przywróć dane Serwera administracyjnego** i kliknij **Dalej**.

6. W kroku **Przywróć ustawienia** kliknij przycisk **Przeglądaj** obok **Folder przechowujący kopie zapasowe**.

7. W otwartym oknie **Zaloguj się do magazynu online** wypełnij następujące pola, a następnie kliknij **OK**:

   - **Nazwa komory S3**

     Nazwa Twojej komory S3.

   - **Folder kopii zapasowej**

     Określ lokalizację folderu magazynu, który jest przeznaczony dla kopii zapasowej.

   - **Identyfikator klucza dostępu**

     Identyfikator klucza dostępu IAM AWS, który należy do użytkownika IAM posiadającego uprawnienia do korzystania z komory S3 (uprawnienie AmazonS3FullAccess).

   - **Tajny klucz**

     Tajny klucz IAM AWS, który należy do użytkownika IAM posiadającego uprawnienia do korzystania z komory S3 (uprawnienie AmazonS3FullAccess).

8. Wybierz opcję **Przenieś z lokalnej kopii zapasowej**. Przycisk **Przeglądaj** stanie się dostępny.

9. Kliknij przycisk **Przeglądaj**, aby wybrać folder na Serwerze administracyjnym AWS, na który skopiowałeś plik backup.zip.

10. Kliknij **Dalej** i zakończ procedurę.

Twoje dane zostaną przywrócone do bazy danych RDS przy użyciu komory S3. Możesz użyć tej bazy danych do dalszej pracy z Kaspersky Security Center w środowisku AWS.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Praca w środowisku chmury Microsoft Azure

Ta sekcja zawiera informacje dotyczące instalacji i obsługi Kaspersky Security Center w środowisku chmury dostarczonym przez Microsoft Azure, a także szczegóły wdrożenia ochrony na maszynach wirtualnych w tym środowisku w chmurze.

W programie Kaspersky Security Center, który został zainstalowany z opcji Usage-based monthly billed SKU, Zarządzanie lukami i poprawkami jest automatycznie aktywowane, a Zarządzanie urządzeniami mobilnymi nie może zostać aktywowane.

Informacje o pracy w Microsoft Azure

Aby pracować z platformą Microsoft Azure, w szczególności, aby kupić aplikacje w Azure Marketplace i utworzyć maszyny wirtualne, będziesz potrzebował subskrypcję Azure. Przed zainstalowaniem Serwera administracyjnego, utwórz ID aplikacji Azure z uprawnieniami wymaganymi do zainstalowania aplikacji na maszynach wirtualnych.

Jeśli kupisz obraz Kaspersky Security Center w sklepie Azure Marketplace, możesz zainstalować maszynę wirtualną z gotowym do użycia Serwerem administracyjnym Kaspersky Security Center. Musisz wybrać ustawienia maszyny wirtualnej, ale nie musisz sam instalować aplikacji. Po instalacji możesz uruchomić Konsolę administracyjną i połączyć się z Serwerem administracyjnym, aby rozpocząć pracę z Kaspersky Security Center.

Możesz również użyć maszyny wirtualnej Azure, na której jest zainstalowany Serwer administracyjny Kaspersky Security Center, aby chronić urządzenia lokalne (na przykład, jeśli serwer chmury okazuje się być łatwiejszy w obsłudze i utrzymaniu niż fizyczny). W takim przypadku możesz pracować z Serwerem administracyjnym tak samo, jak gdyby Serwer administracyjny był zainstalowany na urządzeniu fizycznym. Jeśli nie planujesz korzystać z narzędzi Azure API, nie potrzebujesz ID aplikacji Azure. W tym przypadku subskrypcja Azure jest wystarczająca.

Tworzenie subskrypcji, identyfikatora aplikacji i hasła

Aby pracować z Kaspersky Security Center w środowisku Microsoft Azure, potrzebujesz subskrypcji Azure, ID aplikacji Azure oraz hasła do aplikacji Azure. Możesz użyć istniejącej subskrypcji, jeśli ją posiadasz.

Subskrypcja Azure daje właścicielowi dostęp do portalu Microsoft Azure Platform Management Portal oraz do usług Microsoft Azure. Właściciel może użyć platformy Microsoft Azure Platform do zarządzania usługami takimi, jak Azure SQL i magazyn Azure.

W celu utworzenia subskrypcji Microsoft Azure:

Przejdź na stronę https://account.windowsazure.com/Subscriptions i postępuj zgodnie z dostępnymi tam instrukcjami.

Więcej informacji dotyczących tworzenia subskrypcji można znaleźć na stronie internetowej Microsoft. Uzyskasz ID subskrypcji, który później dostarczysz Kaspersky Security Center wraz z ID aplikacji i hasłem.

W celu utworzenia i zapisania ID aplikacji Azure i hasła:

1. Przejdź do https://portal.azure.com i upewnij się, że jesteś zalogowany.
2. Wykonując instrukcje na stronie referencyjnej, utwórz ID aplikacji.
3. Przejdź do sekcji **Klucze** ustawień aplikacji.
4. W sekcji **Klucze** wypełnij pola **Opis** i **Utraci ważność** i pozostaw pole **Wartość** puste.

5. Kliknij **Zapisz**.

   Jeśli klikniesz **Zapisz**, system automatycznie uzupełni pole **Wartość** długą sekwencją znaków. Ta sekwencja to Twoje hasło do aplikacji Azure (na przykład: yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QIfFvdU=). Opis jest wyświetlany w trakcie wpisywania.

6. Skopiuj hasło i zapisz je, abyś mógł później dostarczyć ID aplikacji i hasło do Kaspersky Security Center.

   Hasło można skopiować, jeśli zostało utworzone. Później hasło nie będzie już wyświetlane i nie będzie można go odzyskać.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Przypisywanie roli do ID aplikacji w Azure

Jeśli chcesz tylko wykrywać maszyny wirtualne przy pomocy wykrywania urządzeń, Twój ID aplikacji Azure musi posiadać rolę Czytelnik. Jeśli chcesz nie tylko wykrywać maszyny wirtualne, ale także wdrożyć ochronę na maszynach wirtualnych, Twój ID aplikacji Azure musi posiadać rolę Współautor maszyny wirtualnej.

Postępuj zgodnie z instrukcjami na stronie internetowej Microsoft, aby przypisać rolę do swojego ID aplikacji Azure.

Instalowanie Serwera administracyjnego w Microsoft Azure i wybieranie bazy danych

W celu zainstalowania Serwera administracyjnego w środowisku Microsoft Azure:

1. Zaloguj się do Microsoft Azure, korzystając ze swojego konta.
2. Przejdź na portal Azure.
3. W lewym panelu kliknij zielony znak plusa.
4. W polu wyszukiwania w menu wpisz „Kaspersky Hybrid Cloud Security”.

   Kaspersky Hybrid Cloud Security to kombinacja Kaspersky Security Center i dwóch aplikacji zabezpieczających do ochrony instancji: Kaspersky Endpoint Security for Linux i Kaspersky Security for Windows Server.

5. Na liście wyników wybierz Kaspersky Hybrid Cloud Security lub Kaspersky Hybrid Cloud Security (BYOL).

   W prawej części okna pojawi się okno z informacjami.

6. Przeczytaj informacje i kliknij przycisk Utwórz u dołu okna z informacjami.
7. Wypełnij wszystkie potrzebne pola. Użyj etykietki narzędzi, aby uzyskać informacje i pomoc.
8. Podczas wybierania rozmiaru wybierz jedną z trzech opcji oznaczonych gwiazdką.

   W większości przypadków wystarcza 8 gigabajtów (GB) pamięci RAM. Jednakże w Azure możesz zwiększyć rozmiar pamięci RAM i inne zasoby maszyny wirtualnej w dowolnym momencie.

9. Podczas wybierania bazy danych wybierz jedną zgodnie ze swoim planem:

- Lokalna—jeśli chcesz bazę danych na tej samej maszynie wirtualnej, na której jest zainstalowany Serwer administracyjny. Kaspersky Security Center jest dostarczany z bazą danych SQL Server Express. Wybierz tę opcję, jeśli SQL Server Express jest wystarczający dla Twoich potrzeb.

- Nowa—jeśli chcesz nową bazę danych RDS w środowisku Azure. Wybierz tę opcję, jeśli chcesz system DBMS inny niż SQL Server Express. Twoje dane zostaną przesłane do środowiska chmury, gdzie pozostaną, i nie będziesz ponosił dodatkowych wydatków.

- Istniejąca—jeśli chcesz, żeby użyć istniejącego serwera bazy danych. W tym przypadku będziesz musiał określić jego lokalizację. Jeśli ten serwer znajduje się poza środowiskiem Azure, Twoje dane zostaną przesłane przez internet, co może generować dodatkowe koszty.

10. Podczas wprowadzania ID subskrypcji użyj subskrypcji, którą utworzyłeś wcześniej.

Po zainstalowaniu, możesz nawiązać połączenie z Serwerem administracyjnym przy użyciu RDP. Do pracy z Serwerem administracyjnym możesz użyć Konsoli administracyjnej.

Praca z Azure SQL

Ta sekcja opisuje działania, jakie mają zostać podjęte w celu przygotowania bazy danych Microsoft Azure dla Kaspersky Security Center, przygotowania konta magazynu Azure, a także przeniesienia istniejącej bazy danych do Azure SQL.

Baza danych SQL jest zarządzaną usługą bazy danych mającą ogólne przeznaczenie w Microsoft Azure.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Tworzenie konta magazynu Azure

Musisz utworzyć konto magazynu w Microsoft Azure do pracy z bazą danych Azure SQL oraz dla skryptów instalacyjnych.

W celu utworzenia konta magazynu:

1. Zaloguj się do portalu Azure.

2. W lewej części okna wybierz **Konta magazynu**, aby przejść do okna **Konta magazynu**.

3. W oknie **Konta magazynu** kliknij przycisk **Dodaj**, aby przejść do okna **Utwórz konto magazynu**.

4. W celu utworzenia konta magazynu wypełnij wszystkie potrzebne pola:

   - Lokalizacja: musi być taka sama jak lokalizacja Serwera administracyjnego.

   - Pozostałe pola: możesz zostawić domyślne wartości.

   Użyj etykietki narzędzi, aby uzyskać informacje o każdym polu.

   Po utworzeniu konta, zostanie wyświetlona lista Twoich kont magazynu.

5. Na liście kont magazynu kliknij nazwę nowo utworzonego konta, aby zobaczyć informacje o tym koncie.

6. Upewnij się, że znasz nazwę konta, grupę zasobu oraz klucze dostępu dla tego konta magazynu. Będziesz potrzebował tych informacji do pracy z Kaspersky Security Center.

Więcej informacji znajdziesz na stronie Azure.

Jeśli już posiadasz konto magazynu, możesz go użyć do pracy z Kaspersky Security Center.

Tworzenie bazy danych Azure SQL i serwera SQL

W środowisku Azure potrzebujesz bazy danych SQL i serwera SQL.

W celu utworzenia bazy danych Azure SQL i serwera SQL:

1. Postępuj zgodnie z instrukcjami na stronie internetowej Azure.

   Możesz utworzyć nowy serwer, gdy Microsoft Azure wyświetli pytanie o wykonanie tego działania; jeśli już masz serwer Azure SQL Server, możesz użyć go dla Kaspersky Security Center niż do utworzenia nowego.

2. Po utworzeniu bazy danych SQL i serwera SQL, upewnij się, że znasz nazwę zasobu i grupę zasobu:

   a. Przejdź do https://portal.azure.com i upewnij się, że jesteś zalogowany.

   b. W lewej części okna wybierz **bazy danych SQL**.

   c. Kliknij nazwę bazy danych z listy swoich baz danych.

      Zostanie otwarte okno właściwości.

   d. Nazwa bazy danych to nazwa zasobu. Nazwa grupy zasobu jest wyświetlana w sekcji **Podgląd** okna właściwości.

Nazwa zasobu i grupa zasobu bazy danych są potrzebne do przeniesienia bazy danych do Azure SQL.

Przenoszenie bazy danych do Azure SQL

Po wdrożeniu Serwera administracyjnego w środowisku Azure, możesz przenieść swoją bazę danych Kaspersky Security Center z lokalnego urządzenia do Azure SQL. Dla bazy danych Azure SQL potrzebne jest konto magazynu Azure. Musisz także posiadać Microsoft SQL Server Data-Tier Application Framework (DacFx) oraz SQLSysCLRTypes na swoim Serwerze administracyjnym.

W celu przeniesienia bazy danych:

1. Upewnij się, że utworzyłeś konto magazynu Azure.

2. Upewnij się, że posiadasz SQLSysCLRTypes i DacFx na swoim Serwerze administracyjnym.

   Możesz pobrać Microsoft SQL Server Data-Tier Application Framework (17.0.1 DacFx) i SQLSysCLRTypes (wybierz wersję odpowiadającą wersji Twojego serwera SQL Server) z oficjalnej strony internetowej Microsoft.

3. Na swoim fizycznym Serwerze administracyjnym (lokalnym) uruchom narzędzie Kaspersky Backup, aby utworzyć kopię zapasową danych Serwera administracyjnego, z włączoną opcją **Wykonaj migrację do formatu Azure**.

4. Skopiuj plik kopii zapasowej na Serwer administracyjny Azure.

   Upewnij się, że posiadasz wystarczającą ilość miejsca na maszynie wirtualnej Azure, na której jest zainstalowany Serwer administracyjny. W środowisku Azure możesz dodać przestrzeń dyskową do swoich maszyn wirtualnych, aby ulokować proces migracji bazy danych.

5. Na Serwerze administracyjnym znajdującym się w środowisku Microsoft Azure uruchom ponownie narzędzie Kaspersky Backup w trybie interaktywnym.

   Zostanie uruchomiony Kreator tworzenia kopii zapasowej i przywracania.

6. W kroku **Wybierz akcję** wybierz **Przywróć dane Serwera administracyjnego** i kliknij **Dalej**.

7. W kroku **Przywróć ustawienia** kliknij przycisk **Przeglądaj** obok **Folder przechowujący kopie zapasowe**.

8. W otwartym oknie **Zaloguj się do magazynu online** wypełnij następujące pola, a następnie kliknij **OK**:

   - **Nazwa konta magazynu Azure**

     Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

   - **Folder kopii zapasowej**

     Określ lokalizację folderu magazynu, który jest przeznaczony dla kopii zapasowej.

   - **ID subskrypcji Azure**

     Subskrypcję utworzyłeś na portalu Azure.

   - **Hasło do aplikacji Azure**

     Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

     Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

   - **Klucz dostępu do magazynu Azure**

     Dostępne we właściwościach Twojego konta magazynu, w sekcji Klucze dostępu. Możesz użyć dowolnego klucza (key1 lub key2).

   - **Nazwa serwera Azure SQL**

     Dostępne we właściwościach Twojego serwera Azure SQL.

   - **Grupa zasobów serwera Azure SQL**

     Dostępne we właściwościach Twojego serwera Azure SQL.

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

9. Wybierz opcję **Przenieś z lokalnej kopii zapasowej**.

   Przycisk **Przeglądaj** stanie się dostępny.

10. Kliknij przycisk **Przeglądaj**, aby wybrać folder na Serwerze administracyjnym Azure, na który skopiowałeś plik kopii zapasowej.

11. Kliknij **Dalej** i zakończ procedurę.

Twoje dane zostaną przywrócone do bazy danych Azure SQL przy użyciu Twojego magazynu Azure. Możesz użyć tej bazy danych do dalszej pracy z Kaspersky Security Center w środowisku Azure.

Adresy stron internetowych cytowane w tym dokumencie są poprawne w dniu wydania Kaspersky Security Center.

Praca w Google Cloud

Ta sekcja zawiera informacje o pracy z Kaspersky Security Center w środowisku chmury udostępnianym przez Google.

Tworzenie adresu e-mail klienta, identyfikatora projektu i klucza prywatnego

Możesz użyć Google API do pracy z Kaspersky Security Center w Google Cloud Platform. Wymagane jest konto Google. Więcej informacji można znaleźć w dokumentacji Google pod adresem https://cloud.google.com.

Konieczne będzie utworzenie i wprowadzenie w Kaspersky Security Center następujących poświadczeń:

- **E-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

Praca z Google Cloud SQL dla instancji MySQL

Możesz utworzyć bazę danych w Google Cloud i używać tej bazy danych dla Kaspersky Security Center.

Kaspersky Security Center współpracuje z MySQL 5.7 i 5.6. Inne wersje MySQL nie zostały przetestowane.

W celu utworzenia i skonfigurowania bazy danych MySQL:

W swojej przeglądarce otwórz stronę https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen i postępuj zgodnie z dostępnymi instrukcjami.

Podczas konfigurowania bazy danych MySQL użyj następujących flag:

- **sort_buffer_size** 10 000 000
- **join_buffer_size** 20 000 000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32 000 000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67 108 864
- **max_heap_table_size** 67 108 864
- **lower_case_table_names** 1

Wymagania wstępne urządzeń klienckich w środowisku chmury niezbędnych do pracy z Kaspersky Security Center

Urządzenia, na których zamierzasz zainstalować Serwer administracyjny, Agenta sieciowego i aplikacje zabezpieczające Kaspersky, muszą spełniać następujące warunki:

- Konfiguracja grup zabezpieczeń udostępnia następujące porty na Serwerze administracyjnym (minimalny zestaw portów wymaganych do wdrożenia):
  - 8060 HTTP—do przesyłania pakietów instalacyjnych Agenta sieciowego i pakietów instalacyjnych aplikacji zabezpieczających z Serwera administracyjnego na chronione instancje
  - 8061 HTTPS — do przesyłania pakietów instalacyjnych Agenta sieciowego i pakietów instalacyjnych aplikacji zabezpieczających z Serwera administracyjnego na chronione instancje
  - 13000 TCP—dla przesyłania z chronionych instancji i podrzędnych Serwerów administracyjnych do głównego Serwera administracyjnego przy użyciu SSL

- 13000 UDP—do przesyłania informacji o zamknięciu instancji na Serwer administracyjny
- 14000 TCP—dla przesyłania z chronionych instancji i podrzędnych Serwerów administracyjnych do głównego Serwera administracyjnego bez użycia SSL
- 13291—do łączenia Konsoli administracyjnej z Serwerem administracyjnym
- 40080—do działania skryptów instalacyjnych

Możesz skonfigurować grupy bezpieczeństwa w konsoli AWS Management Console lub na portalu Azure. Jeśli zamierzasz używać Kaspersky Security Center w niedomyślnej konfiguracji, zapoznaj się z Bazą wiedzy. Przykłady niedomyślnej konfiguracji obejmują nie instalowanie Konsoli administracyjnej na Serwerze administracyjnym, ale zainstalowanie jej na stacji roboczej lub przy pomocy serwera proxy KSN.

- Port UDP o numerze 15000 jest dostępny na urządzeniach klienckich (do odbierania żądań komunikacji z Serwerem administracyjnym).
- W środowisku chmury AWS:
  - Jeśli planujesz korzystać z AWS API, ustawiona jest rola IAM, pod którą aplikacje zostaną zainstalowane na instancjach.
  - Na każdej instancji Amazon EC2 zainstalowany i uruchomiony jest Agent SSM (Systems Manager Agent).
  - Agent SSM umożliwia Kaspersky Security Center automatyczne instalowanie aplikacji na urządzeniach i grupach urządzeń bez wyświetlania pytania o potwierdzenie administratora za każdym razem.
  - Na instancjach, na których jest zainstalowany system operacyjny Windows i które zostały wdrożone z obrazów AMI później niż w listopadzie 2016 roku, agent SSM jest zainstalowany i uruchomiony. Na wszystkich pozostałych urządzeniach należy ręcznie zainstalować agenta SSM. Więcej informacji na temat instalowania agenta SSM na urządzeniach działających pod kontrolą systemów operacyjnych Windows i Linux można znaleźć na stronie pomocy AWS.
- W środowisku chmury Microsoft Azure:
  - Na każdej maszynie wirtualnej Azure zainstalowany i uruchomiony jest Agent Azure VM.

    Domyślnie, nowa maszyna wirtualna jest tworzona z Agentem Azure VM i nie musisz go ręcznie instalować ani włączać. Więcej informacji o Agencie Azure VM znajdziesz w pomocy firmy Microsoft dla urządzeń Windows i urządzeń Linux.
  - Twój ID aplikacji Azure posiada następujące role:
    - Czytelnik (do wykrywania maszyn wirtualnych przy użyciu przeszukiwania)
    - Współautor maszyny wirtualnej (do wdrażania ochrony na maszynach wirtualnych)
    - Współautor serwera SQL (do używania bazy danych SQL w środowisku Microsoft Azure)

    Jeśli chcesz wykonywać wszystkie te działania, przypisz wszystkie trzy role do swojego ID aplikacji Azure.

Tworzenie pakietów instalacyjnych wymaganych do konfiguracji środowiska chmury

Kreator konfiguracji środowiska chmury w Kaspersky Security Center jest dostępny, jeśli masz pakiety instalacyjne i wtyczki administracyjne dla następujących programów:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

  > Wdrożenie Kaspersky Endpoint Security for Windows w środowisku chmurowym będzie dostępne po nadchodzącej wersji Kaspersky Endpoint Security 11.12 for Windows.

- Kaspersky Security for Windows Server

Te pakiety instalacyjne są wymagane do zainstalowania aplikacji na instancjach lub maszynach wirtualnych, które chcesz chronić. Jeśli nie masz tych pakietów instalacyjnych, musisz je utworzyć. W przeciwnym razie Kreator konfiguracji środowiska chmury nie będzie działać.

W celu utworzenia pakietów instalacyjnych:

1. Pobierz najnowsze wersje aplikacji i wtyczek ze strony internetowej Kaspersky:
   - Instalator i wtyczkę zarządzającą dla Kaspersky Security for Windows Server.
   - Instalator, pliki dla zdalnej instalacji za pośrednictwem Kaspersky Security Center oraz wtyczkę zarządzającą dla Kaspersky Endpoint Security for Linux.
2. Zapisz wszystkie pliki na instancji (lub maszynie wirtualnej), na której jest zainstalowany Serwer administracyjny.
3. Wyodrębnij pliki ze wszystkich pakietów.
4. Uruchom Kaspersky Security Center.
5. W drzewie konsoli przejdź do **Zaawansowane** → **Zdalna instalacja** → **Pakiety instalacyjne** i kliknij **Utwórz pakiet instalacyjny**.
6. Wybierz **Utwórz pakiet instalacyjny Kaspersky**.
7. Określ nazwę pakietu i ścieżkę do instalatora aplikacji: <folder>\<nazwa pliku>.kud, a następnie kliknij **Dalej**.
8. Przeczytaj Umowę licencyjną i zaznacz pole potwierdzające, że zaakceptowałeś jej warunki, a następnie kliknij **Dalej**.

Pakiet instalacyjny zostanie przesłany na Serwer administracyjny i będzie dostępny na liście pakietów instalacyjnych.

Konfiguracja środowiska chmury stanie się dostępna, gdy tylko utworzysz pakiety instalacyjne i zainstalujesz wtyczki administracyjne na Serwerze administracyjnym.

Konfigurowanie środowiska chmury

Aby skonfigurować Kaspersky Security Center przy użyciu Kreatora konfiguracji środowiska chmury, musisz mieć:

- Następujące dane uwierzytelniające środowiska w chmurze:

    - Rolę IAM, której udzielono uprawnienie do przeszukiwania segmentu chmury lub konto użytkownika IAM, któremu udzielono uprawnienia do przeszukiwania segmentu chmury (do pracy z Amazon Web Services)
    - ID aplikacji Azure, hasło i subskrypcję (do pracy z Microsoft Azure)
    - Poczta klienta Google, ID projektu i klucz prywatny (do pracy z Google Cloud)
- Pakiety instalacyjne:
    - Agent sieciowy dla systemu Windows
    - Agent sieciowy dla systemu Linux
    - Kaspersky Endpoint Security for Linux
- Wtyczka sieciowa dla Kaspersky Endpoint Security for Linux
- Wybierz jeden z następujących:
    - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Endpoint Security for Windows (zalecane)
    - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Security for Windows Server

Jeśli nie chcesz używać funkcji środowiska chmury (na przykład, jeśli chcesz zarządzać ochroną jedynie fizycznych urządzeń klienckich), możesz zamknąć Kreatora konfiguracji środowiska chmury i ręcznie uruchomić standardowego Kreatora wstępnej konfiguracji Serwera administracyjnego.

Operacja Konfigurowanie środowiska chmury uruchamia się automatycznie przy pierwszym połączeniu z Serwerem administracyjnym za pośrednictwem Konsoli administracyjnej, jeśli instalujesz Kaspersky Security Center z gotowego do użycia obrazu. Kreator konfiguracji środowiska chmury można również uruchomić ręcznie w dowolnym momencie.

Aby ręcznie uruchomić Kreatora konfiguracji środowiska chmury:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.
2. Z menu kontekstowego węzła wybierz **All Tasks** → **Konfiguruj środowisko chmury**.

Średni czas pracy wynosi około 15 minut.

Informacje o Kreatorze konfiguracji środowiska chmury

Kreator konfiguracji środowiska chmury umożliwia skonfigurowanie Kaspersky Security Center z uwzględnieniem specyfiki pracy w środowisku chmury.

kreator tworzy następujące obiekty:

- Profil Agenta sieciowego z ustawieniami domyślnymi
- Profil dla Kaspersky Endpoint Security for Linux
- Profil dla Kaspersky Security for Windows Server

- Grupa administracyjna dla instancji i reguła dla automatycznego przenoszenia instancji do tej grupy administracyjnej
- Zadanie tworzenia kopii zapasowej danych Serwera administracyjnego
- Zadania instalowania ochrony na urządzeniach działających pod kontrolą systemu Linux i Windows
- Zadania dla każdego zarządzanego urządzenia:
  - Szybkie skanowanie w poszukiwaniu złośliwego oprogramowania
  - Pobieranie uaktualnień

Jeśli wybrano opcję licencjonowania BYOL, konfigurowanie środowiska chmury aktywuje również Kaspersky Security Center za pomocą pliku klucza lub kodu aktywacyjnego i umieszcza plik klucza lub kod aktywacyjny w magazynie licencji.

Krok 1. Wybieranie metody aktywacji aplikacji

Ten krok nie jest wyświetlany, jeśli zarejestrowano się dla jednego z gotowych do użycia obrazów AMI (w AWS Marketplace) lub dla opcji Usage-based monthly billed SKU (w Azure Marketplace). W takim przypadku kreator natychmiast przechodzi do następnego kroku. Jednakże nie możesz kupić gotowego do użycia obrazu AMI dla Google Cloud.

Jeśli wybrałeś opcję licencjonowania BYOL dla Kaspersky Security Center, kreator wyświetli pytanie o wybór metody aktywacji aplikacji.

Aktywuj aplikację przy użyciu kodu aktywacyjnego / pliku klucza dla Kaspersky Security for Virtualization lub dla Kaspersky Hybrid Cloud Security.

Możesz aktywować aplikację w jeden z następujących sposobów:

- Wprowadzając kod aktywacyjny.

  Rozpocznie się aktywacja online. Ten proces będzie obejmował weryfikację określonego kodu aktywacyjnego, a także wydanie i aktywację pliku klucza.

- Określając plik klucza.

  Aplikacja sprawdzi plik klucza i dokona aktywacji, jeśli zawiera poprawne informacje, lub wyświetli okno z prośbą o określenie innego pliku klucza.

Kaspersky Security Center umieszcza klucz licencyjny w magazynie licencji i oznacza go jako klucz rozsyłany automatycznie na zarządzane urządzenia.

Jeśli łączysz się z instancją przy użyciu standardowego Podłączania pulpitu zdalnego w Microsoft Windows lub podobnej aplikacji, we właściwościach połączenia zdalnego należy określić napęd urządzenia fizycznego, którego używasz do nawiązania połączenia. Zapewnia to dostęp z instancji do plików na urządzeniu fizycznym oraz pozwala wybrać i określić plik klucza.

Podczas pracy z Kaspersky Security Center zainstalowanym z płatnego obrazu AMI lub dla Usage-based monthly billed SKU nie można dodawać plików kluczy lub kodów aktywacyjnych do magazynu licencji.

Krok 2. Wybieranie środowiska chmury

Wybierz środowisko chmury, w którym instalujesz Kaspersky Security Center: AWS, Azure lub Google Cloud.

Krok 3. Autoryzacja w środowisku chmury

AWS

Jeśli wybrałeś AWS, określ, czy posiadasz rolę IAM z wymaganymi uprawnieniami, lub zapewnij Kaspersky Security Center klucz dostępu IAM AWS. Przeszukiwanie segmentu chmury nie jest możliwe bez roli IAM lub klucza dostępu IAM AWS.

Skonfiguruj następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment”, „AWS Segment” lub „Google Segment”.

- **Użyj roli AWS IAM**

  Wybierz tę opcję, jeśli już utworzyłeś rolę IAM dla Serwera administracyjnego do korzystania z usług AWS.

- **Użyj konta użytkownika AWS IAM**

  Wybierz tę opcję, jeśli posiadasz konto użytkownika IAM z wymaganymi uprawnieniami oraz możesz wprowadzić ID klucza oraz tajny klucz.

  - **Identyfikator klucza dostępu**

    Identyfikator klucza dostępu IAM to sekwencja znaków alfanumerycznych. Identyfikator klucza otrzymałeś podczas tworzenia konta użytkownika IAM.

    Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

  - **Tajny klucz**

Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

To połączenie zostanie zapisane w ustawieniach aplikacji. Możesz utworzyć tylko jeden klucz dostępu AWS IAM za pomocą konfiguracji środowiska chmury. Możesz określić więcej połączeń do zarządzania innymi segmentami chmury.

Jeśli chcesz zainstalować aplikacje na instancjach poprzez Kaspersky Security Center, upewnij się, że Twoja rola IAM (lub użytkownik IAM, którego konto jest skojarzone z wprowadzanym kluczem) posiada wszystkie wymagane uprawnienia.

Azure

Jeśli wybrałeś Azure, skonfiguruj następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment”, „AWS Segment” lub „Google Segment”.

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **ID subskrypcji Azure**

  Subskrypcję utworzyłeś na portalu Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **Klucz dostępu do magazynu Azure**

  Hasło (klucz) uzyskałeś po utworzeniu konta magazynu Azure do pracy z Kaspersky Security Center.

  Klucz jest dostępny w sekcji „Overview of the Azure storage account", w podsekcji „Keys".

To połączenie zostanie zapisane w ustawieniach aplikacji.

Google Cloud

Jeśli wybrałeś Google Cloud, określ następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

- **E-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

To połączenie zostanie zapisane w ustawieniach aplikacji.

Krok 4. Konfigurowanie synchronizacji z chmurą i wybieranie dalszych działań

W tym kroku rozpoczyna się przeszukiwanie segmentu chmury i tworzona jest grupa administracyjna dla instancji. Instancje, wykryte podczas przeszukiwania, zostają umieszczone w tej grupie. Konfigurowany jest terminarz przeszukiwania segmentu chmury (domyślnie, co 5 minut).

Tworzona jest także reguła automatycznego przydzielania **Synchronizuj z chmurą**. Dla każdego kolejnego skanowania sieci chmury, wykryte urządzenia wirtualne zostaną przeniesione do odpowiedniej podgrupy w obrębie grupy **Zarządzane urządzenia\Chmura**.

W oknie **Synchronizacja z segmentem chmury** możesz zdefiniować następujące ustawienia:

- **Synchronizuj strukturę grupy administracyjnej z segmentem chmury**

  Jeśli ta opcja jest włączona, grupa **Chmura** jest automatycznie tworzona w obrębie grupy **Zarządzane urządzenia** oraz zostaje uruchomione wyszukiwanie urządzeń w chmurze. Instancje i maszyny wirtualne, które zostały wykryte w trakcie każdego skanowania sieci chmury, zostają umieszczone w grupie Chmura. Struktura podgrup administracyjnych w obrębie tej grupy odpowiada strukturze Twojego segmentu chmury (w AWS, strefy dostępności i grupy położenia nie są przedstawione w strukturze; w Azure, podsieci nie są przedstawione w strukturze). Urządzenia, które nie zostały zidentyfikowane jako instancje w środowisku chmury, znajdują się w grupie **Urządzenia nieprzypisane**. Struktura grupa umożliwia korzystanie z grupowych zadań instalacji do zainstalowania aplikacji antywirusowych na instancjach, a także skonfigurowanie różnych zasad dla różnych grup.

  Jeśli ta opcja jest wyłączona, tworzona jest także grupa **Chmura** oraz uruchamiane jest wyszukiwanie urządzeń; jednakże podgrupy odpowiadające strukturze segmentu chmury nie są tworzone w obrębie tej grupy. Wszystkie wykryte instancje znajdują się w grupie administracyjnej **Chmura**, więc są wyświetlane na jednej liście. Jeśli Twoja praca z Kaspersky Security Center wymaga synchronizacji, możesz zmodyfikować właściwości reguły **Synchronizuj z chmurą** i wymusić ją. Wymuszenie tej reguły zmieni strukturę podgrup w grupie Chmura tak, że będzie ona odpowiadała strukturze segmentu chmury.

  Domyślnie opcja ta jest wyłączona.

- **Roześlij ochronę**

  Jeśli ta opcja jest zaznaczona, kreator tworzy zadanie instalacji aplikacji zabezpieczających na instancjach. Po zakończeniu pracy kreatora, na urządzeniach w Twoich segmentach chmury automatycznie uruchamiany jest Kreator wdrażania ochrony, dzięki czemu możliwe będzie zainstalowanie Agenta sieciowego i aplikacji zabezpieczających na tych urządzeniach.

  Kaspersky Security Center może przeprowadzić zdalną instalację przy użyciu swoich narzędzi. Jeśli nie masz uprawnień do instalowania aplikacji na instancjach EC2 lub maszynach wirtualnych Azure, możesz ręcznie skonfigurować zadanie **Zdalna instalacja** oraz określić konto z wymaganymi uprawnieniami. W tym przypadku, zadanie Zdalna instalacja nie będzie działało dl urządzeń wykrytych przy użyciu AWS API lub Azure. To zadanie będzie działało tylko dla urządzeń wykrytych przy użyciu przeszukiwania Active Directory, przeszukiwania domeny Windows lub przeszukiwania zakresu IP.

  Jeśli ta opcja nie jest zaznaczona, Kreator wdrażania ochrony nie zostanie uruchomiony, a zadania instalacji aplikacji zabezpieczających na instancjach nie zostaną utworzone. Te działania można wykonać ręcznie w późniejszym czasie.

W przypadku Google Cloud możesz przeprowadzić tylko zdalną instalację natywnych narzędzi Kaspersky Security Center. Jeśli wybrałeś Google Cloud, opcja **Roześlij ochronę** nie jest dostępna.

Krok 5. Konfigurowanie Kaspersky Security Network w środowisku chmury

Określ ustawienia przekazywania informacji o działaniach Kaspersky Security Center do bazy wiedzy Kaspersky Security Network. Wybierz jedną z następujących opcji:

- **Zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje zainstalowane na urządzeniach klienckich automatycznie prześlą szczegóły swoich działań do Kaspersky Security Network. Uczestnictwo w Kaspersky Security Network umożliwia szybsze aktualizowanie baz danych zawierających informacje o wirusach i innych zagrożeniach, co zapewnia szybszą reakcję na pojawiające się zagrożenia bezpieczeństwa.

- Nie zgadzam się na korzystanie z Kaspersky Security Network

  Kaspersky Security Center i zarządzane aplikacje nie dostarczą informacji do Kaspersky Security Network.

  Jeśli wybierzesz tę opcję, korzystanie z Kaspersky Security Network zostanie wyłączone.

Kaspersky zaleca uczestniczenie w Kaspersky Security Network.

Krok 6. Konfigurowanie powiadomień e-mail w środowisku chmury

Skonfiguruj dostarczanie powiadomień o zdarzeniach zarejestrowanych podczas działania aplikacji firmy Kaspersky na wirtualnych urządzeniach klienckich. Ustawienia te będą używane jako ustawienia domyślne dla profili aplikacji.

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w aplikacjach firmy Kaspersky użyj następujących ustawień:

- Adresaci (adresy e-mail)

  Adresy e-mail użytkowników, którym aplikacja będzie wysyłała powiadomienia. Możesz wprowadzić jeden lub więcej adresów; jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami.

- Serwery SMTP

  Adres lub adresy serwerów pocztowych Twojej organizacji.

  Jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami. Możesz użyć następujących wartości:

  - Adres IPv4 lub IPv6
  - Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
  - Nazwa DNS serwera SMTP

- Port serwera SMTP

  Numer portu komunikacji serwera SMTP. Jeśli korzystasz z kilku serwerów SMTP, połączenie z nimi jest nawiązywane przez określony port komunikacyjny. Domyślny numer portu to 25.

- Użyj uwierzytelniania ESMTP

  Włącza obsługę autoryzacji ESMTP. Po zaznaczeniu opcji, w polach **Nazwa użytkownika** i **Hasło** możesz określić ustawienia autoryzacji ESMTP. Domyślnie pole to nie jest zaznaczone.

Możesz przetestować nowe ustawienia powiadomień e-mail, klikając przycisk **Wyślij wiadomość testową**. Jeśli wiadomość testowa została pomyślnie odebrana przez odbiorców, których adresy zostały określone w polu **Adresaci (adresy e-mail)**, oznacza to, że ustawienia zostały poprawnie skonfigurowane.

Krok 7. Tworzenie wstępnej konfiguracji ochrony środowiska chmury

W tym kroku Kaspersky Security Center automatycznie tworzy profile i zadania. Okno **Konfiguracja wstępnej ochrony** wyświetla listę profili i zadań utworzonych przez aplikację.

Jeśli używasz bazy danych RDS w środowisku chmury AWS, podczas tworzenia zadania wykonywania kopii zapasowej Serwera administracyjnego musisz dostarczyć parę kluczy dostępu IAM do Kaspersky Security Center. W tym przypadku wypełnij następujące pola:

- **Nazwa komory S3**

  Nazwa komory S3, którą utworzyłeś dla Kopii zapasowej.

- **Identyfikator klucza dostępu**

  Identyfikator klucza (sekwencja znaków alfanumerycznych) uzyskałeś podczas tworzenia konta użytkownika IAM do pracy z instancją magazynu komory S3.

  Pole jest dostępne, jeśli w komorze S3 wybrałeś bazę danych RDS.

- **Tajny klucz**

  Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

  Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

  Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

Jeśli używasz bazy danych Azure SQL w środowisku chmury Azure, podczas tworzenia zadania wykonywania kopii zapasowej Serwera administracyjnego musisz dostarczyć informacje o serwerze Azure SQL do Kaspersky Security Center. W tym przypadku wypełnij następujące pola:

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **ID subskrypcji Azure**

  Subskrypcję utworzyłeś na portalu Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **Nazwa serwera Azure SQL**

  Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

- **Grupa zasobów serwera Azure SQL**

  Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

- **Klucz dostępu do magazynu Azure**

  Dostępne we właściwościach Twojego konta magazynu, w sekcji Klucze dostępu. Możesz użyć dowolnego klucza (key1 lub key2).

Jeśli instalujesz Serwer administracyjny w Google Cloud, musisz wybrać folder, w którym będą przechowywane kopie zapasowe. Wybierz folder na swoim dysku lokalnym lub folder na instancji maszyny wirtualnej.

Przycisk **Dalej** stanie się dostępny po utworzeniu wszystkich profili i zadań, które są niezbędne dla minimalnej konfiguracji ochrony.

Jeśli urządzenie, na którym zadania powinny zostać uruchomione, nie jest widoczne dla Serwera administracyjnego, zadania zostaną uruchomione dopiero wtedy, gdy urządzenie stanie się widoczne. Jeśli tworzysz nową instancję EC2 lub nową maszynę wirtualną, może zająć trochę czasu zanim stanie się widoczna dla Serwera administracyjnego. Jeśli chcesz, żeby Agent sieciowy i aplikacje zabezpieczające zostali zainstalowani na wszystkich nowo utworzonych urządzeń tak szybko, jak to możliwe, Upewnij się, że opcja **Uruchom pominięte zadania** jest włączona dla zadań **Zdalna instalacja aplikacji**. W przeciwnym razie nowo utworzona instancja / maszyna wirtualna nie uzyska Agenta sieciowego i aplikacji zabezpieczających, dopóki zadanie nie zostanie uruchomione zgodnie z jej terminarzem.

Krok 8. Wybieranie działania, jeśli system operacyjny musi być uruchomiony ponownie podczas instalacji (dla środowiska chmury)

Jeśli wcześniej wybrałeś **Roześlij ochronę**, musisz wybrać, co zrobić, gdy system operacyjny urządzenia docelowego musi zostać uruchomiony ponownie. Jeśli nie wybrałeś opcji **Roześlij ochronę**, ten krok zostanie pominięty.

Wybierz, czy instancje powinny być uruchamiane ponownie, jeśli system operacyjny urządzenia musi być uruchomiony ponownie podczas instalacji aplikacji:

- **Nie uruchamiaj urządzenia ponownie**

  Jeśli ta opcja jest zaznaczona, urządzenie nie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

- **Uruchom urządzenie ponownie**

  Jeśli ta opcja jest zaznaczona, urządzenie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

Jeśli chcesz wymusić zamknięcie wszystkich aplikacji w zablokowanych sesjach na instancjach przed ponownym uruchomieniem, zaznacz pole **Wymuś zamknięcie aplikacji dla zablokowanych sesji**. Jeśli to pole jest odznaczone, będziesz musiał ręcznie zamknąć wszystkie aplikacje działające na zablokowanych instancjach.

Krok 9. Pobieranie uaktualnień przez Serwer administracyjny

W tym kroku możesz zobaczyć postęp pobierania uaktualnień niezbędnych do prawidłowego działania Serwera administracyjnego. Możesz kliknąć przycisk **Dalej** bez czekania na zakończenie pobierania, aby przejść do ostatniego okna kreatora.

kreator zakończy swoje działanie.

Sprawdzanie konfiguracji

W celu sprawdzenia, czy Kaspersky Security Center 14.2 został poprawnie skonfigurowany do pracy w środowisku chmury:

1. Uruchom Kaspersky Security Center i upewnij się, że możesz nawiązać połączenie z Serwerem administracyjnym poprzez Konsolę administracyjną.
2. Z drzewa konsoli wybierz folder **Zarządzane urządzenia\Chmura**.
3. Podczas przeglądania dowolnej podgrupy w grupie **Zarządzane urządzenia\Chmura** upewnij się, że zakładka **Urządzenia** wyświetla wszystkie urządzenia tej podgrupy.

   Jeśli urządzenia nie są wyświetlane, możesz ręcznie przeszukać odpowiednie segmenty chmury, aby je odnaleźć.
4. Upewnij się, że na zakładce **Zasady** są aktywne profile dla następujących aplikacji:
   - Agent sieciowy Kaspersky Security Center
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   Jeśli ich nie ma, możesz je utworzyć ręcznie.
5. Upewnij się, że zakładka **Zadania** wyświetla następujące zadania:
   - **Tworzenie kopii zapasowych danych Serwera administracyjnego**
   - **Zadanie aktualizacji dla Windows Server**
   - **Konserwacja baz danych**
   - **Pobierz aktualizacje do repozytorium Serwera administracyjnego**
   - **Wyszukaj luki i wymagane aktualizacje**
   - **Zainstaluj ochronę dla systemu Windows**
   - **Zainstaluj ochronę dla systemu Linux**

- **Zadanie Szybkie skanowanie dla Windows Server**
- **Szybkie skanowanie**
- **Zainstaluj aktualizacje dla systemu Linux**

Jeśli ich nie ma, możesz je utworzyć ręcznie.

Program Kaspersky Security Center 14.2 został poprawnie skonfigurowany do pracy w środowisku chmury.

Grupa urządzeń w chmurze

Możesz zarządzać urządzeniami w chmurze, łącząc je w grupy. Na etapie wstępnej konfiguracji Kaspersky Security Center, grupa administracyjna **Zarządzane urządzenia\Chmura** jest tworzona domyślnie, a urządzenia w chmurze, wykryte podczas przeszukiwania, zostają umieszczone w tej grupie.

Jeśli po skonfigurowaniu synchronizacji wybrałeś opcję **Synchronizuj strukturę grupy administracyjnej z segmentem chmury**, struktura podgrup w tej grupie administracyjnej jest identyczna jak struktura segmentów chmury (jednakże w AWS strefy dostępności i grupy położenia nie są przedstawione w strukturze; w Microsoft Azure podsieci nie są przedstawione w strukturze). Puste podgrupy w obrębie grupy, które są wykrywane podczas przeszukiwania, są automatycznie usuwane.

Możesz także ręcznie utworzyć grupy administracyjne, łącząc wszystkie lub określone urządzenia.

Domyślnie, grupa **Zarządzane urządzenia\Chmura** dziedziczy zasady i zadania od grupy **Zarządzane urządzenia**. Możesz zmienić ustawienia, jeśli pola **Edytowanie dozwolone** zostały zaznaczone we właściwościach ustawień odpowiednich profili i zadań.

Przeszukiwanie segmentu sieci

Informacje o strukturze sieci i urządzeniach w tej sieci są otrzymywane przez Serwer administracyjny poprzez regularne przeszukiwanie segmentów chmury przy pomocy narzędzi AWS API, Azure API lub Google API. Kaspersky Security Center używa tych informacji do aktualizacji zawartości folderów: **Urządzenia nieprzypisane** i **Zarządzane urządzenia**. Jeżeli skonfigurowałeś automatyczne przenoszenie urządzeń do grup administracyjnych, wykryte urządzenia zostaną włączone do grup administracyjnych.

Aby zezwolić Serwerowi administracyjnemu na przeszukiwanie segmentów chmury, musisz posiadać uprawnienia dla roli IAM lub dla konta użytkownika IAM (w AWS) lub przy pomocy hasła i ID aplikacji (w Azure) lub przy pomocy poczty klienta Google, identyfikatora projektu Google i klucza prywatnego.

Możesz dodawać i usuwać połączenia, a także ustawić terminarz przeszukiwania dla każdego segmentu chmury.

Dodawanie połączeń dla przeszukiwania segmentu chmury

W celu dodania połączenia dla przeszukiwania segmentu chmury do listy dostępnych połączeń:

1. W drzewie konsoli wybierz węzeł **Wykrywanie urządzeń** → **Chmura**.

2. W obszarze roboczym okna kliknij **Konfiguruj przeszukiwanie**.

   Zostanie otwarte okno właściwości zawierające listę połączeń dostępnych dla przeszukiwania segmentu chmury.

3. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Połączenie**.

4. Określ nazwę środowiska chmury dla połączenia, która będzie używana do dalszego przeszukiwania segmentu chmury:

   Środowisko chmury

   Środowiskiem, w którym znajdują się instancje EC2 / maszyny wirtualne, mogą być Amazon Web Services (AWS), Microsoft Azure lub Google Cloud.

   Jeśli wybrałeś AWS, określ następujące ustawienia:

   - **Nazwa połączenia**

     Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

     Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

     Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

   - **Użyj roli AWS IAM**

     Wybierz tę opcję, jeśli już utworzyłeś rolę IAM dla Serwera administracyjnego do korzystania z usług AWS.

   - **Użyj konta użytkownika AWS IAM**

     Wybierz tę opcję, jeśli posiadasz konto użytkownika IAM z wymaganymi uprawnieniami oraz możesz wprowadzić ID klucza oraz tajny klucz.

     - **Identyfikator klucza dostępu**

       Identyfikator klucza dostępu IAM to sekwencja znaków alfanumerycznych. Identyfikator klucza otrzymałeś podczas tworzenia konta użytkownika IAM.

       Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

     - **Tajny klucz**

       Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

       Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

       Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

Kreator konfiguracji środowiska chmury umożliwia określenie tylko jednego klucza dostępu AWS IAM. Możesz określić więcej połączeń do zarządzania innymi segmentami chmury.

Jeśli wybrałeś Azure, określ następujące ustawienia:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **ID subskrypcji Azure**

  Subskrypcję utworzyłeś na portalu Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **Klucz dostępu do magazynu Azure**

  Hasło (klucz) uzyskałeś po utworzeniu konta magazynu Azure do pracy z Kaspersky Security Center.

  Klucz jest dostępny w sekcji „Overview of the Azure storage account", w podsekcji „Keys".

Jeśli wybrałeś Google Cloud, określ następujące ustawienia:

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment", „AWS Segment" lub „Google Segment".

- **E-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

5. Jeśli chcesz, wybierz **Ustaw terminarz przeszukiwania** i zmień ustawienia domyślne.

   To połączenie zostanie zapisane w ustawieniach aplikacji.

Po pierwszym przeszukaniu nowego segmentu chmury, w grupie administracyjnej **Zarządzane urządzenia\Chmura** pojawi się podgrupa odpowiadająca temu segmentowi.

Jeśli określisz niepoprawne dane uwierzytelniające, podczas przeszukiwania segmentu chmury nie zostaną wykryte żadne instancje, a nowa podgrupa nie pojawi się w grupie administracyjnej **Zarządzane urządzenia\Chmura**.

Usuwanie połączeń dla przeszukiwania segmentu chmury

Jeśli już nie chcesz przeszukiwać określonego segmentu chmury, możesz usunąć połączenie odpowiadające temu segmentowi z listy dostępnych połączeń. Połączenie można usunąć także wtedy, gdy, na przykład, uprawnienia do przeszukiwania segmentu chmury zostały przeniesione na innego użytkownika AWS IAM z innym kluczem.

W celu usunięcia połączenia:

1. W drzewie konsoli wybierz węzeł **Wykrywanie urządzeń → Chmura**.
2. W obszarze roboczym okna wybierz **Konfiguruj przeszukiwanie**.

   Zostanie otwarte okno zawierające listę połączeń dostępnych dla przeszukiwania segmentu chmury.
3. Wybierz połączenie, które chcesz usunąć, i kliknij przycisk **Usuń** dostępny w prawej części okna.
4. W otwartym oknie kliknij przycisk **OK**, aby potwierdzić swój wybór.

Jeśli usuwasz połączenia z listy dostępnych połączeń, urządzenia, które znajdują się w obrębie odpowiednich segmentów, są automatycznie usuwane z odpowiednich grup administracyjnych.

Konfigurowanie terminarza przeszukiwania

Przeszukiwanie segmentu chmury odbywa się zgodnie z terminarzem. Możesz ustawić częstotliwość przeszukiwania.

Częstotliwość przeszukiwania jest automatycznie ustawiana na 5 minut w ustawieniach konfiguracji środowiska chmury. Możesz zmienić tę wartość w dowolnym momencie i ustawić inny terminarz. Nie jest zalecane konfigurowanie wykonywania przeszukiwania z częstotliwością większą niż co 5 minut, ponieważ może to prowadzić do błędów w działaniu AWS API.

W celu skonfigurowania terminarza przeszukiwania segmentu chmury:

1. W drzewie konsoli wybierz węzeł **Wykrywanie urządzeń** → **Chmura**.
2. W obszarze roboczym kliknij **Konfiguruj przeszukiwanie**.

   Zostanie otwarte okno właściwości chmury.
3. Na liście wybierz żądane połączenie i kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości połączenia.
4. W oknie właściwości kliknij odnośnik **Określ terminarz przeszukiwania**.

   Zostanie otwarte okno **Terminarz**.
5. Określ następujące ustawienia:

   - **Zaplanowane uruchomienie**

     Dostępne są następujące opcje terminarza przeszukiwania:

     - Co N dni

       Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

       Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

     - Co N minut

       Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

       Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

     - Według dni tygodnia

       Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

       Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

     - Co miesiąc, w określone dni wybranych tygodni

       Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

       Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest włączona.

6. Kliknij **OK**, aby zachować zmiany.

Terminarz przeszukiwania zostaje skonfigurowany i zapisany.

Instalowanie aplikacji na urządzeniach w środowisku chmury

Na urządzeniach w środowisku chmury możesz zainstalować następujące aplikacje firmy Kaspersky: Kaspersky Security for Windows Server (dla urządzeń Windows) i Kaspersky Endpoint Security for Linux (dla urządzeń Linux).

Urządzenia klienckie, na których chcesz wdrożyć ochronę, muszą spełniać wymagania do działania Kaspersky Security Center w środowisku chmury. Aby zainstalować aplikacje na instancjach AWS, na instancjach maszyn wirtualnych Microsoft Azure lub maszyn wirtualnych Google, musisz posiadać ważną licencję.

Kaspersky Security Center 14.2 obsługuje następujące scenariusze:

- Urządzenie klienckie jest wykrywane przy użyciu API; instalacja odbywa się również przy użyciu API. Ten scenariusz jest obsługiwany dla środowisk w chmurze AWS i Azure.
- Urządzenie klienckie zostaje wykryte przy użyciu przeszukiwania Active Directory, przeszukiwania domen Windows lub przeszukiwania zakresu IP; instalacja odbywa się przy użyciu Kaspersky Security Center.
- Urządzenie klienckie jest wykrywane przy użyciu Google API; instalacja odbywa się przy użyciu Kaspersky Security Center. W przypadku Google Cloud tylko ten scenariusz jest obsługiwany.

Inne sposoby instalacji aplikacji nie są obsługiwane.

Aby zainstalować aplikacje na urządzeniach wirtualnych, użyj pakietów instalacyjnych.

W celu utworzenia zadania zdalnej instalacji aplikacji na instancjach przy użyciu AWS API lub Azure API:

1. Z drzewa konsoli wybierz folder **Zadania**.
2. Kliknij przycisk **Nowe zadanie**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.
3. W oknie **Wybierz typ zadania** jako typ zadania wybierz **Zdalna instalacja aplikacji**.
4. W oknie **Wybierz urządzenia**, z grupy **Zarządzane urządzenia\Chmura** wybierz odpowiednie urządzenia.

5. Jeśli Agent sieciowy nie został jeszcze zainstalowany na urządzeniach, na których zamierzasz zainstalować aplikację, w kroku **Wybieranie konta do uruchomienia zadania** wybierz **Konto wymagane (Agent sieciowy nie jest używany)** i kliknij przycisk **Dodaj** dostępny w prawej części okna. Z menu, które zostanie wyświetlone, wybierz jedną z następujących opcji:

   - **Konto w chmurze**

     Wybierz tę opcję, jeśli chcesz zainstalować aplikacje na instancjach w AWS i posiadasz klucz dostępu IAM AWS z wymaganymi uprawnieniami, ale nie posiadasz roli IAM. Dodatkowo, wybierz tę opcję, jeśli chcesz zainstalować aplikacje na urządzeniach w środowisku Azure.

     W otwartym oknie zapewnij Kaspersky Security Center poświadczenia, które nadają uprawnienia do instalowania aplikacji na odpowiednich urządzeniach.

     Wybierz środowisko chmury: AWS lub Azure.

     W polu **Nazwa konta** wprowadź nazwę dla tych poświadczeń. Ta nazwa pojawi się na liście kont do uruchomienia zadania.

     Jeśli wybrałeś AWS, w polach **Identyfikator klucza dostępu** i **Klucz tajny** wprowadź poświadczenia dla konta użytkownika IAM, który posiada uprawnienia do zainstalowania aplikacji na określonych urządzeniach.

     Jeśli wybrałeś Azure, w polach **ID subskrypcji Azure** i **Hasło do aplikacji Azure** wprowadź poświadczenia dla konta Azure, który posiada uprawnienia do zainstalowania aplikacji na określonych urządzeniach.

     Jeśli określisz niepoprawne poświadczenia, zadanie zdalnej instalacji zakończy się błędem na urządzeniach, dla których zostało to zaplanowane.

   - **Konto**

     W przypadku instancji działających pod kontrolą systemu Windows, wybierz tę opcję, jeśli nie chcesz zainstalować aplikacji przy użyciu narzędzi AWS lub Azure API. W tym przypadku upewnij się, że urządzenia w Twoim segmencie chmury spełniają potrzebne warunki. Kaspersky Security Center sam instaluje aplikacje, bez użycia AWS API lub Azure API.

     Jeśli określisz niepoprawne dane, zadanie zdalnej instalacji zakończy się błędem na urządzeniach, dla których zostało to zaplanowane.

   - **Rola IAM**

     Wybierz tę opcję, jeśli chcesz zainstalować aplikacje na instancjach w środowisku AWS i posiadasz rolę IAM z wymaganymi uprawnieniami.

     Jeśli wybierzesz tę opcję, ale nie posiadasz roli IAM z wymaganymi uprawnieniami, zadanie zdalnej instalacji zakończy się błędem na urządzeniach, dla których zostało to zaplanowane.

   - **Certyfikat SSH**

W przypadku instancji działających pod kontrolą systemu Linux, wybierz tę opcję, jeśli nie chcesz zainstalować aplikacji przy użyciu narzędzi AWS API lub Azure API. W tym przypadku upewnij się, że urządzenia w Twoim segmencie chmury spełniają potrzebne warunki. Kaspersky Security Center sam instaluje aplikacje, bez użycia AWS API lub Azure API.

Aby określić klucz prywatny certyfikatu SSH, możesz go wygenerować za pomocą narzędzia ssh-keygen. Należy zauważyć, że Kaspersky Security Center obsługuje format PEM kluczy prywatnych, ale narzędzie ssh-keygen domyślnie generuje klucze SSH w formacie OPENSSH. Format OPENSSH nie jest obsługiwany przez Kaspersky Security Center. Aby utworzyć klucz prywatny w obsługiwanym formacie PEM, dodaj opcję `-m PEM` w poleceniu ssh-keygen. Na przykład:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "< adres e-mail użytkownika >"
```

Możesz udostępnić kilka poświadczeń, klikając przycisk **Dodaj** za każdym razem, gdy chcesz dodać poświadczenia. Jeśli różne segmenty chmury wymagają różnych poświadczeń, zapewnij poświadczenia dla wszystkich segmentów.

Po zakończeniu pracy kreatora, zadanie zdalnej instalacji aplikacji pojawi się na liście zadań w obszarze roboczym folderu **Zadania**.

W Microsoft Azure zdalna instalacja aplikacji zabezpieczających na maszynie wirtualnej może spowodować usunięcie niestandardowego rozszerzenia skryptu, zainstalowanego na maszynie wirtualnej.

Przeglądanie właściwości urządzeń w chmurze

W celu przejrzenia właściwości urządzenia w chmurze:

1. W drzewie konsoli, w węźle **Wykrywanie urządzeń** → **Chmura** wybierz podwęzeł odpowiadający grupie, w której znajduje się odpowiednia instancja.

   Jeśli nie wiesz, w jakiej grupie znajduje się odpowiednie urządzenie wirtualne, skorzystaj z funkcji wyszukiwania:

   a. Kliknij prawym klawiszem myszy nazwę węzła **Zarządzane urządzenia** → **Cloud**, a następnie, z menu kontekstowego wybierz **Szukaj**.

   b. W otwartym oknie przeprowadź wyszukiwanie.

      Jeśli istnieje urządzenie, które odpowiada ustawionym kryteriom, jego nazwa i szczegóły zostaną wyświetlone w dolnej części okna.

2. Kliknij nazwę odpowiedniego węzła prawym klawiszem myszy. Z menu kontekstowego wybierz **Właściwości**.

   W otwartym oknie zostaną wyświetlone właściwości obiektu.

   Sekcja **Informacje o systemie** → **Ogólne informacje o systemie** zawiera właściwości, które są specyficzne dla urządzeń w środowisku chmury:

   - **Urządzenie wykryte za pomocą interfejsu API** (**AWS**, **Azure** lub **Google Cloud**; jeśli urządzenia nie można wykryć za pomocą narzędzi API, wyświetlana jest wartość **No** - Nie).
   - **Region chmury**.
   - **Cloud VPC** (tylko dla urządzeń AWS i Google Cloud).

- **Strefa dostępności w chmurze** (tylko dla urządzeń AWS i Google Cloud).
- **Podsieć chmury**.
- **Grupa położenia w chmurze** (ta jednostka jest wyświetlana tylko wtedy, gdy instancja należy do grupy położenia; w innym przypadku nie jest wyświetlana).

Możesz kliknąć przycisk **Eksportuj do pliku**, aby wyeksportować te informacje do pliku .csv lub .txt.

Synchronizacja z chmurą

Podczas operacji Konfiguruj środowisko chmurowe automatycznie tworzona jest reguła Synchronizuj z chmurą. Ta reguła umożliwia automatyczne przenoszenie instancji, wykrytych przy każdym przeszukiwaniu, z grupy **Urządzenia nieprzypisane** do grupy **Zarządzane urządzenia\Chmura**, aby te instancje stały się dostępne dla scentralizowanego zarządzania. Domyślnie, reguła jest aktywna po utworzeniu. Regułę można wyłączyć, zmodyfikować lub wymusić w dowolnym momencie.

W celu zmodyfikowania właściwości reguły Synchronizuj z chmurą i/lub wymuszenia reguły:

1. W drzewie konsoli kliknij prawym klawiszem myszy nazwę węzła **Wykrywanie urządzeń**.
2. Z menu kontekstowego wybierz **Właściwości**.
3. W otwartym oknie **właściwości**, w panelu **Sekcje** wybierz **Przenieś urządzenia**.
4. Na liście reguł przenoszenia urządzeń w obszarze roboczym wybierz **Synchronizuj z chmurą**, a następnie kliknij przycisk **Właściwości**, znajdujący się w dolnej części okna.

   Zostanie otwarte okno właściwości reguły.
5. W razie potrzeby określ następujące ustawienia w grupie ustawień **Segmenty chmury**:
   - Urządzenie znajduje się w segmencie chmury

     Reguła jest tylko stosowana do urządzeń, które znajdują się w wybranym segmencie chmury. W innej sytuacji reguła będzie stosowana do wszystkich urządzeń, które zostały wykryte.

     Domyślnie opcja ta jest zaznaczona.
     - Włączając obiekty potomne

       Reguła będzie stosowana do wszystkich urządzeń w wybranym segmencie i we wszystkich zagnieżdżonych podsekcjach chmury. W innym przypadku reguła jest tylko stosowana do urządzeń, które znajdują się w głównym segmencie.

       Domyślnie opcja ta jest zaznaczona.
     - Przenieś urządzenia z obiektów zagnieżdżonych do odpowiednich podgrup

Jeśli ta opcja jest włączona, urządzenia z obiektów zagnieżdżonych zostaną automatycznie przeniesione do podgrup, które odpowiadają ich strukturze.

Jeśli ta opcja jest wyłączona, urządzenia z obiektów zagnieżdżonych zostaną automatycznie przeniesione do głównej podgrupy Chmura bez dalszego rozdzielania.

Domyślnie opcja ta jest włączona.

- Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń

  Jeśli ta opcja jest włączona, gdy struktura grupy **Zarządzane urządzenia\Chmura** nie posiada podgrup, które będą odpowiadały sekcji zawierającej urządzenie, Kaspersky Security Center utworzy takie podgrupy. Na przykład, jeśli nowa podsieć zostanie wykryta podczas wyszukiwania urządzeń, nowa grupa z taką samą nazwą zostanie utworzona w grupie **Zarządzane urządzenia\Chmura**.

  Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie tworzy żadnych nowych podgrup. Na przykład, jeśli nowa podsieć zostanie wykryta podczas przeszukiwania sieci, nowa grupa o tej samej nazwie nie zostanie utworzona w grupie **Zarządzane urządzenia\Chmura**, a urządzenia, które są w tej podsieci, zostaną przeniesione do grupy **Zarządzane urządzenia\Chmura**.

  Domyślnie opcja ta jest włączona.

- Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury

  Jeśli ta opcja jest włączona, aplikacja usunie z grupy Chmura wszystkie podgrupy, które nie odpowiadają żadnym istniejącym obiektom chmury.

  Jeśli ta opcja jest wyłączona, podgrupy, które nie odpowiadają żadnym istniejącym obiektom chmury, zostaną zachowane.

  Domyślnie opcja ta jest włączona.

Jeśli podczas działania środowiska **Konfiguruj chmurę** włączono opcję **Synchronizuj z chmurą**, reguła **Synchronizuj z chmurą zostanie utworzona z wybranymi opcjami** Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń i Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury.

Jeśli nie włączyłeś opcji **Synchronizuj z chmurą**, reguła Synchronizuj z chmurą zostanie utworzona z wyłączonymi (odznaczonymi) tymi opcjami. Jeśli Twoja praca z Kaspersky Security Center wymaga, aby struktura podgrup w podgrupie **Zarządzane urządzenia\Chmura** odpowiadała strukturze segmentów chmury, włącz opcje **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń** i **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury** we właściwościach reguły, a następnie wymuś regułę.

6. Z listy rozwijalnej **Urządzenie odnalezione przy użyciu API** wybierz jedną z następujących wartości:
   - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.
   - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.
   - **Google Cloud.** Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku Google Cloud.
   - **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale nie może zostać wykryte przy użyciu API.

7. **Brak wartości**. Warunek nie ma zastosowania. Jeśli to konieczne, skonfiguruj inne właściwości reguły w innych sekcjach.

8. Jeśli to konieczne, wymuś regułę, klikając przycisk **Wymuś** znajdujący się w dolnej części okna.

   Zostanie uruchomiony Kreator wykonywania reguły. Postępuj zgodnie z instrukcjami kreatora. Jeśli kreator zakończy swoje działanie, reguła zostanie uruchomiona, a struktura podgrup w podgrupie **Zarządzane urządzenia\Chmura** będzie odpowiadała strukturze segmentów chmury.

9. Kliknij przycisk **OK**.

Właściwości zostały skonfigurowane i zapisane.

W celu wyłączenia reguły Synchronizuj z chmura:

1. W drzewie konsoli kliknij prawym klawiszem myszy nazwę węzła **Wykrywanie urządzeń**.

2. Z menu kontekstowego wybierz **Właściwości**.

3. W otwartym oknie **właściwości**, w panelu **Sekcje** wybierz **Przenieś urządzenia**.

4. Na liście reguł przenoszenia urządzeń w obszarze roboczym wyłącz (odznacz) opcję **Synchronizuj z chmurą** i kliknij **OK**.

Reguła zostanie wyłączona i nie będzie już stosowana.

Używanie skryptów instalacyjnych do zdalnej instalacji aplikacji zabezpieczających

Jeśli Kaspersky Security Center jest wdrożony w środowisku chmury, możesz użyć skryptów instalacyjnych do automatycznego wdrażania aplikacji zabezpieczających. Skrypty instalacyjne dla Amazon Web Services, Microsoft Azure i Google Cloud są dostępne w plikach ZIP na stronie pomocy technicznej Kaspersky.

Możesz wdrożyć najnowsze wersje Kaspersky Endpoint Security for Linux i Kaspersky Security for Windows Server przy użyciu skryptów instalacyjnych tylko wtedy, gdy już utworzyłeś pakiety instalacyjne i wtyczki zarządzające dla tych programów. Aby wdrożyć najnowsze wersje aplikacji zabezpieczających przy użyciu skryptów instalacyjnych, na Serwerze administracyjnym w środowisku chmury wykonaj następujące czynności:

1. Uruchom działanie Konfiguruj środowisko chmury.

2. Postępuj zgodnie z instrukcjami podanymi na stronie https://support.kaspersky.com/14713.

Wdrożenie Kaspersky Security Center w Yandex.Cloud

Możesz wdrożyć Kaspersky Security Center w Yandex.Cloud. Dostępny jest tylko tryb płatności za użycie; bazy danych w chmurze nie są obsługiwane.

W Yandex.Cloud dostępne są następujące metody wdrażania aplikacji zabezpieczających:

- Przy użyciu podstawowej metody programu Kaspersky Security Center, to znaczy poprzez zadanie *Zdalna instalacja* (wdrażanie programów zabezpieczających jest możliwe tylko wtedy, gdy Serwer administracyjny i

maszyny wirtualne, które mają być chronione, znajdują się w tym samym segmencie sieci)

- Za pomocą skryptów instalacji

Aby zainstalować Kaspersky Security Center w Yandex.Cloud, musisz mieć konto usługi w Yandex.Cloud. Musisz nadać temu kontu uprawnienie marketplace.meteringAgent i powiązać to konto z maszyną wirtualną (szczegółowe informacje można znaleźć na stronie https://cloud.yandex.com/en).

Dodatki

Ta sekcja zawiera dodatkowe informacje i fakty związane z korzystaniem z Kaspersky Security Center.

Zaawansowane funkcje

Ta sekcja opisuje zakres dodatkowych opcji Kaspersky Security Center zaprojektowanych do poszerzenia funkcjonalności scentralizowanego zarządzania aplikacjami na urządzeniach.

Automatyzacja działania Kaspersky Security Center. Narzędzie klakaut

Możesz zautomatyzować działanie Kaspersky Security Center przy użyciu narzędzia klakaut. Narzędzie klakaut i jego system pomocy znajdują się w folderze instalacyjnym Kaspersky Security Center.

Narzędzia niestandardowe

Kaspersky Security Center umożliwia utworzenie listy *narzędzi niestandardowych* (zwanych dalej również *narzędziami*), czyli aplikacji aktywowanych dla urządzenia klienckiego w Konsoli administracyjnej przy użyciu grupy **Narzędzia użytkownika** z menu kontekstowego. Każde narzędzie na liście będzie skojarzone z oddzielnym poleceniem menu, którego Konsola administracyjna używa do uruchomienia aplikacji odpowiadającej temu narzędziu.

Aplikacja jest uruchamiana na stacji roboczej administratora. Aplikacja może akceptować atrybuty zdalnego urządzenia klienckiego jako argumenty wiersza poleceń (nazwa NetBIOS, nazwa DNS lub adres IP). Połączenie ze zdalnym urządzeniem można nawiązać przy użyciu połączenia tunelowego.

Domyślnie, lista narzędzi niestandardowych zawiera następujące usługi dla każdego urządzenia klienckiego:

- **Zdalna diagnostyka** to narzędzie do zdalnej diagnostyki programu Kaspersky Security Center.
- **Zdalny pulpit** to standardowy składnik systemu Microsoft Windows o nazwie Podłączanie pulpitu zdalnego.
- **Zarządzanie komputerem** to standardowy komponent systemu Microsoft Windows.

W celu dodania lub usunięcia narzędzi niestandardowych, bądź też zmodyfikowania ich ustawień:

Z menu kontekstowego urządzenia klienckiego wybierz **Narzędzia użytkownika** → **Konfiguruj narzędzia użytkownika**.

Zostanie otwarte okno **Narzędzia użytkownika**. W tym oknie możesz dodawać niestandardowe narzędzia lub edytować ich ustawienia za pomocą przycisków **Dodaj** i **Modyfikuj**. Aby usunąć narzędzie niestandardowe, kliknij przycisk usuwania z ikoną czerwonego krzyżyka ( ).

Tryb klonowania dysku Agenta sieciowego

Klonowanie dysku twardego odpowiedniego urządzenia jest popularną metodą instalacji oprogramowania na nowych urządzeniach. Jeśli Agent sieciowy jest uruchomiony w trybie standardowym na dysku twardym odpowiedniego urządzenia, mogą pojawić się następujące problemy:

Po zainstalowaniu odpowiedniego obrazu dysku przy pomocy Agenta sieciowego na nowych urządzeniach, będą one wyświetlane jako pojedyncza ikona w Konsoli administracyjnej. Ten problem pojawia się, ponieważ procedura klonowania powoduje, że nowe urządzenia przechowują identyczne dane wewnętrzne, które umożliwiają Serwerowi administracyjnemu skojarzenie urządzenia z ikoną w Konsoli administracyjnej.

Specjalny *tryb klonowania dysku Agenta sieciowego* umożliwia uniknięcie problemów z nieprawidłowym wyświetlaniem nowych urządzeń w Konsoli administracyjnej po klonowaniu. Użyj tego trybu podczas instalowania oprogramowania (z Agentem Sieciowym) na nowych urządzeniach za pomocą klonowania dysku.

W trybie klonowania dysku Agent sieciowy pracuje cały czas, ale nie łączy się z Serwerem administracyjnym. Po wyjściu z trybu klonowania, Agent sieciowy usuwa dane wewnętrzne, które umożliwiają Serwerowi administracyjnemu skojarzenie kilku urządzeń z jedną ikona w Konsoli administracyjnej. Po zakończeniu klonowania obrazu odpowiedniego urządzenia, nowe urządzenia są wyświetlane w Konsoli administracyjnej prawidłowo (z indywidualnymi ikonami).

Scenariusz użycia trybu klonowania dysku Agenta sieciowego

1. Administrator instaluje Agenta sieciowego na odpowiednim urządzeniu.
2. Administrator sprawdza połączenie Agenta sieciowego z Serwerem administracyjnym przy użyciu narzędzia klnagchk.
3. Administrator włącza tryb klonowania dysku Agenta sieciowego.
4. Administrator instaluje oprogramowanie i łaty na urządzeniu i uruchamia je ponownie niezbędną ilość razy.
5. Administrator klonuje dysk twardy odpowiedniego urządzenia na dowolnej liczbie urządzeń.
6. Każda sklonowana kopia musi spełniać następujące warunki:
    a. Nazwa urządzenia musi być zmieniona.
    b. Urządzenie musi zostać uruchomione ponownie.
    c. Tryb klonowania dysku musi być wyłączony.

Włączanie i wyłączanie trybu klonowania dysku przy użyciu narzędzia klmover

W celu włączenia / wyłączenia trybu klonowania dysku Agenta sieciowego:

1. Uruchom narzędzie klmover na urządzeniu z zainstalowanym Agentem sieciowym, które potrzebujesz sklonować.

Narzędzie klmover znajduje się w folderze instalacyjnym Agenta sieciowego.

2. W celu włączenia trybu klonowania dysku, w wierszu poleceń systemu Windows wprowadź następujące polecenie: `klmover -cloningmode 1`.

   Agent sieciowy przełączy się do trybu klonowania dysku.

3. W celu uzyskania bieżącego stanu trybu klonowania dysku, w wierszu poleceń wprowadź następujące polecenie: `klmover -cloningmode`.

   Okno narzędzia wskaże, czy tryb klonowania dysku jest włączony czy wyłączony.

4. W celu wyłączenia trybu klonowania dysku, w wierszu poleceń narzędzia wprowadź następujące polecenie: `klmover -cloningmode 0`.

Przygotowywanie urządzenia referencyjnego z zainstalowanym Agentem sieciowym do utworzenia obrazu systemu operacyjnego

Możesz chcieć utworzyć obraz systemu operacyjnego urządzenia referencyjnego z zainstalowanym Agentem sieciowym, a następnie wdrożyć obraz na urządzeniach w sieci. W tym przypadku możesz utworzyć obraz systemu operacyjnego urządzenia referencyjnego, na którym Agent sieciowy nie został jeszcze uruchomiony. Jeśli uruchomisz Agenta sieciowego na urządzeniu referencyjnym przed utworzeniem obrazu systemu operacyjnego, identyfikacja urządzeń wdrożonych z obrazu systemu operacyjnego urządzenia referencyjnego przez Serwer administracyjny będzie problematyczna.

W celu przygotowania urządzenia referencyjnego do utworzenia obrazu systemu operacyjnego:

1. Upewnij się, że system operacyjny Windows jest zainstalowany na urządzeniu referencyjnym i zainstaluj inne oprogramowanie, którego potrzebujesz na tym urządzeniu.

2. Na urządzeniu referencyjnym, w ustawieniach Połączenia sieciowe systemu Windows odłącz urządzenie referencyjne od sieci, w której zainstalowany jest program Kaspersky Security Center.

3. Na urządzeniu referencyjnym uruchom lokalną instalację Agenta sieciowego przy pomocy pliku setup.exe.

   Zostanie uruchomiony kreator instalacji Agenta sieciowego Kaspersky Security Center. Postępuj zgodnie z instrukcjami kreatora.

4. Na stronie **Serwer administracyjny** kreatora określ adres IP Serwera administracyjnego.

   Jeśli nie znasz dokładnego adresu Serwera administracyjnego, wprowadź localhost. Możesz zmienić adres IP w późniejszym czasie, korzystając z narzędzia klmover z przełącznikiem `-address`.

5. W kroku **Uruchom aplikację** wyłącz opcję **Uruchom aplikację podczas instalacji**.

6. Po zakończeniu instalacji Agenta sieciowego, nie uruchamiaj urządzenia przed utworzeniem obrazu systemu operacyjnego.

   Jeśli uruchomisz urządzenie ponownie, będziesz musiał powtórzyć cały proces przygotowania urządzenia referencyjnego przed utworzeniem obrazu systemu operacyjnego.

7. Na urządzeniu referencyjnym, w wierszu polecenia uruchom narzędzie sysprep i wykonaj następujące polecenie: `sysprep.exe /generalize /oobe /shutdown`.

Urządzenie referencyjne jest gotowe do utworzenia obrazu systemu operacyjnego.

Konfigurowanie odbierania wiadomości od komponentu Monitor integralności pliku

Zarządzane aplikacje, takie jak Kaspersky Security for Windows Server lub Kaspersky Security for Virtualization Light Agent wysyłają wiadomości z Monitora integralności plików do Kaspersky Security Center. Kaspersky Security Center umożliwia także monitorowanie wszelkich zmian wprowadzonych w ogromnie ważnych komponentach systemów (np. Serwery sieciowe i ATM) i natychmiastowe reagowanie na naruszenie integralności tych systemów. Dlatego też możesz otrzymywać wiadomości z komponentu Monitor integralności plików. Komponent Monitor integralności plików umożliwia monitorowanie nie tylko systemu plików urządzenia, ale także gałęzi rejestru, stanu zapory sieciowej i stanu podłączonego sprzętu.

Należy skonfigurować Kaspersky Security Center do odbierania wiadomości od komponentu Monitor integralności plików bez używania Kaspersky Security for Windows Server lub Kaspersky Security for Virtualization Light Agent.

W celu skonfigurowania odbierania wiadomości od komponentu Monitor integralności plików:

1. Otwórz rejestr systemu urządzenia, na którym jest zainstalowany Serwer administracyjny (na przykład lokalnie, przy użyciu polecenia regedit z poziomu menu **Start** → **Uruchom**).

2. Przejdź do gałęzi:

   - W systemach 32-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - W systemach 64-bitowych:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Utwórz klucze:

   - Utwórz klucz KLSRV_EVP_FIM_PERIOD_SEC, aby określić przedział czasu dla zliczania liczby przetwarzanych zdarzeń. Określ następujące ustawienia:

     a. Jako nazwę klucza określ KLSRV_EVP_FIM_PERIOD_SEC.

     b. Jako typ klucza określ DWORD.

     c. Określ zakres wartości dla przedziału czasu od 43 200 do 172 800 sekund. Domyślnie przedział czasu wynosi 86 400 sekundy.

   - Utwórz klucz KLSRV_EVP_FIM_LIMIT, aby ograniczyć liczbę otrzymanych zdarzeń dla określonego przedziału czasu. Określ następujące ustawienia:

     a. Jako nazwę klucza określ KLSRV_EVP_FIM_LIMIT.

     b. Jako typ klucza określ DWORD.

     c. Określ zakres wartości dla otrzymanych zdarzeń od 2 000 do 50 000. Domyślna liczba zdarzeń to 20 000.

   - Utwórz klucz KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC, aby zliczać zdarzenia z dokładnością do określonego przedziału czasu. Określ następujące ustawienia:

     a. Jako nazwę klucza określ KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC.

b. Jako typ klucza określ DWORD.

c. Określ zakres wartości od 120 do 600 sekund. Domyślny przedział czasu wynosi 300 sekund.

- Utwórz klucz KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC, aby, po minięciu określonego przedziału czasu, aplikacja mogła sprawdzić, czy liczba zdarzeń przetworzonych w określonym przedziale czasu jest mniejsza niż wskazany limit. To sprawdzanie odbywa się po osiągnięciu limitu liczby otrzymanych zdarzeń. Jeśli ten warunek jest spełniony, aplikacja wznowi zapisywanie zdarzeń w bazie danych. Określ następujące ustawienia:

  a. Jako nazwę klucza określ KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC.

  b. Jako typ klucza określ DWORD.

  c. Określ zakres wartości od 600 do 3 600 sekund. Domyślny przedział czasu wynosi 1 800 sekund.

Jeśli klucze nie zostaną utworzone, używane będą wartości domyślne.

4. Uruchom ponownie usługę Serwera administracyjnego.

Ograniczenia dotyczące liczby otrzymywanych zdarzeń od komponentu Monitor integralności plików zostaną skonfigurowane. Wyniki działania komponentu Monitor integralności plików można przejrzeć w raportach: **10 najważniejszych reguł Monitora integralności plików / Monitorowania integralności systemu, które były najczęściej wywoływane na urządzeniach** and **10 urządzeń z najczęściej wywołanymi regułami Monitora integralności plików / Monitorowania integralności systemu**.

Konserwacja Serwera administracyjnego

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

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

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

Zadanie *Konserwacja Serwera administracyjnego* obsługuje wersję MariaDB 10.3 i nowsze. Jeśli używasz MariaDB w wersji 10.2 lub wcześniejszej, administratorzy muszą samodzielnie utrzymywać ten DBMS.

W celu utworzenia zadania Konserwacja Serwera administracyjnego:

1. W drzewie konsoli należy wybrać węzeł Serwera administracyjnego, dla którego chcesz utworzyć zadanie *Konserwacja Serwera administracyjnego*.
2. Wybierz folder **Zadania**.
3. Kliknij przycisk **Nowe zadanie** w obszarze roboczym folderu **Zadania**.

Zostanie uruchomiony Kreator tworzenia nowego zadania.

4. W oknie **Wybierz typ zadania** kreatora jako typ zadania wybierz **Konserwacja Serwera administracyjnego** i kliknij **Dalej**.

5. Jeśli podczas konserwacji musisz zmniejszyć bazę danych Serwera administracyjnego, w oknie **Ustawienia** zaznacz pole **Zmniejsz bazę danych**.

6. Wykonaj pozostałe instrukcje kreatora.

Nowo utworzone zadanie będzie wyświetlane na liście zadań, w obszarze roboczym folderu **Zadania**. Dla jednego Serwera administracyjnego można uruchomić tylko jedno zadanie *Konserwacja Serwera administracyjnego*. Jeśli zadanie *Konserwacja Serwera administracyjnego* zostało już utworzone dla Serwera administracyjnego, nie będzie można utworzyć nowego zadania *Konserwacja Serwera administracyjnego*.

Dostęp do publicznych serwerów DNS

Jeśli dostęp do serwerów Kaspersky przy użyciu systemowego DNS nie jest możliwy, Kaspersky Security Center może korzystać z tych publicznych serwerów DNS w następującej kolejności:

1. Google Public DNS (8.8.8.8)

2. Cloudflare DNS (1.1.1.1)

3. Alibaba Cloud DNS (223.6.6.6)

4. Quad9 DNS (9.9.9.9)

5. CleanBrowsing (185.228.168.168)

Żądania kierowane do tych serwerów DNS mogą zawierać adresy domen oraz publiczny adres IP Serwera administracyjnego, ponieważ aplikacja nawiązuje połączenie TCP/UDP z serwerem DNS. Jeśli Kaspersky Security Center korzysta z publicznego serwera DNS, przetwarzanie danych podlega polityce prywatności odpowiedniej usługi. Aby wyłączyć korzystanie z publicznego DNS, użyj narzędzia klscflag i wprowadź następujące polecenie, korzystając z uprawnień administratora:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
```

Aby go ponownie włączyć, wprowadź następujące polecenie, korzystając z uprawnień administratora:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
```

Okno Metoda powiadamiania użytkownika

W oknie **Metoda powiadamiania użytkownika** możesz skonfigurować powiadamianie użytkownika o instalacji certyfikatu na urządzeniu mobilnym:

- **Pokaż odnośnik w kreatorze**. Jeśli wybierzesz tę opcję, łącze do pakietu instalacyjnego zostanie wyświetlone w ostatnim kroku kreatora połączeń urządzenia mobilnego.

- **Wyślij odnośnik do użytkownika**. Jeśli wybierzesz tę opcję, możesz określić ustawienia powiadamiania użytkownika o podłączeniu urządzenia.

W tej grupie ustawień **Przez e-mail** możesz skonfigurować powiadamianie użytkownika o instalacji nowego certyfikatu na jego urządzeniu mobilnym za pośrednictwem wiadomości e-mail. Ta metoda powiadamiania jest dostępna tylko wtedy, gdy opcja Serwer SMTP jest włączona.

W grupie ustawień **Przez SMS** możesz skonfigurować powiadamianie użytkownika o instalacji certyfikatu na jego urządzeniu mobilnym za pośrednictwem wiadomości SMS. Ta metoda powiadamiania jest dostępna tylko wtedy, gdy opcja Powiadomienia SMS jest włączona.

Kliknij odnośnik **Edytuj wiadomość** w grupach ustawień **Przez e-mail** i **Przez SMS**, aby wyświetlić i edytować powiadomienie (jeśli to konieczne).

Sekcja Ogólne

W tej sekcji możesz dostosować ogólne ustawienia profilu dla urządzeń mobilnych Exchange ActiveSync:

- **Nazwa**

  Nazwa profilu.

- **Akceptuj niezabezpieczone urządzenia**

  Jeśli ta opcja jest włączona, urządzenia, które nie mogą uzyskać dostępu do wszystkich ustawień zasady Exchange ActiveSync, mogą nawiązywać połączenie z serwerem urządzeń mobilnych. Korzystając z połączenia, możesz zarządzać urządzeniami mobilnymi Exchange ActiveSync. Na przykład, możesz ustawić hasła, skonfigurować wysyłanie wiadomości e-mail lub wyświetlić informacje o urządzeniach, takie jak identyfikator urządzenia lub stan zasad.

  Jeśli ta opcja jest wyłączona, nie można połączyć się z serwerem urządzeń mobilnych i zarządzać urządzeniami mobilnymi Exchange ActiveSync.

  Domyślnie opcja ta jest włączona. Możesz wyłączyć tę opcję, jeśli nie zamierzasz zarządzać urządzeniami mobilnymi Exchange ActiveSync i otrzymywać o nich informacji.

- **Częstotliwość aktualizacji (godziny)**

  Jeśli ta opcja jest włączona, aplikacja odświeża informacje o zasadzie Exchange ActiveSync z częstotliwością podaną w polu wejściowym.

  Jeśli opcja jest wyłączona, informacje o zasadzie Exchange ActiveSync nie są odświeżane.

  Domyślnie ta opcja jest włączona, a informacje są odświeżane co godzinę.

Okno Wybór urządzeń

Wskaż wybór na liście **Wybór urządzeń**. Lista zawiera domyślne wybory oraz wybory utworzone przez użytkownika.

Możesz wyświetlić szczegóły wyborów urządzeń w obszarze roboczym sekcji **Wybory urządzeń**.

Okno Określ nazwę nowego obiektu

W oknie określ nazwę nowo utworzonego obiektu. Nazwa nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).

Sekcja Kategorie aplikacji

W tej sekcji możesz skonfigurować dystrybucję informacji o kategoriach aplikacji na urządzenia klienckie.

Pełna transmisja danych (dla Agentów sieciowych w wersji Service Pack 2 i starszych)

Jeśli ta opcja jest zaznaczona, wszystkie dane z kategorii aplikacji będą przekazywane do urządzeń klienckich, jeśli ta kategoria została zmodyfikowana. Ta opcja przekazywania danych używana jest z Network Agent Service Pack 2 lub z wcześniejszymi wersjami.

Transmisja tylko zmodyfikowanych danych (dla Agenta sieciowego w wersji Service Pack 2 i nowszej)

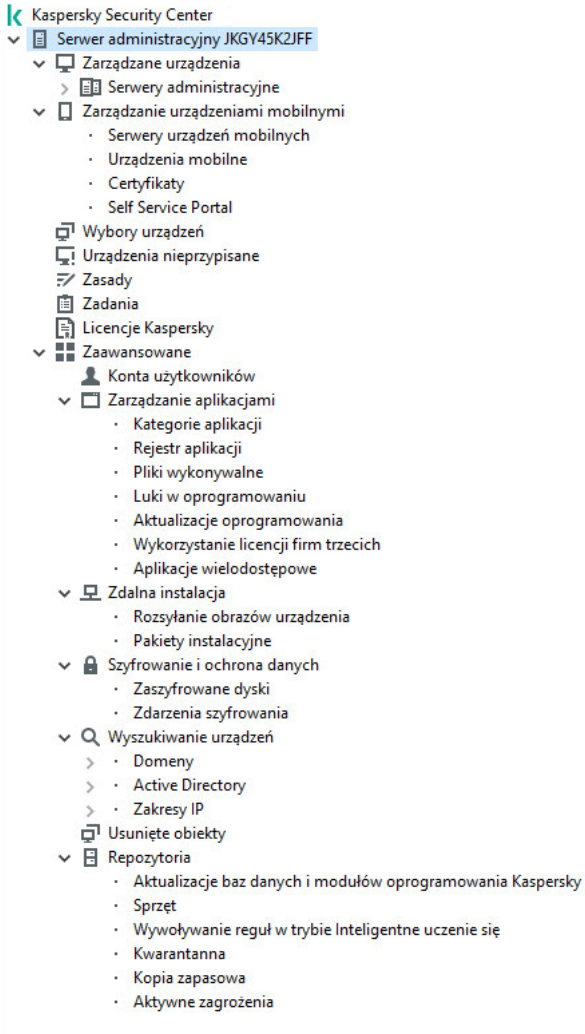
Jeśli ta opcja jest zaznaczona, w momencie modyfikacji kategorii aplikacji, tylko zmodyfikowane dane zostaną przekazane na urządzenia klienckie. Ta opcja przekazywania danych jest używana z Network Agent Service Pack 2 i późniejszymi wersjami.

Funkcje korzystania z interfejsu do zarządzania

Ta sekcja opisuje działania, które można wykonać w oknie głównym Kaspersky Security Center.

Drzewo konsoli

Drzewo konsoli (patrz poniższy rysunek) wyświetla hierarchię Serwerów administracyjnych, które znajdują się w sieci firmowej, strukturę ich grup administracyjnych i inne obiekty aplikacji, takie jak foldery **Repozytoria** lub **Zarządzanie aplikacjami**. Obszar nazw Kaspersky Security Center może zawierać kilka węzłów, włączając nazwy serwerów odpowiadające zainstalowanym Serwerom administracyjnym będącym częścią hierarchii.



Drzewo konsoli

Węzeł Serwer administracyjny

Węzeł **Serwer administracyjny – <Nazwa urządzenia>** jest kontenerem odzwierciedlającym strukturę folderów wybranego Serwera administracyjnego.

Obszar roboczy węzła **Serwer administracyjny** zawiera informacje podsumowujące o bieżącym stanie aplikacji i urządzeń zarządzanych przez Serwer administracyjny. Informacje w obszarze roboczym zostały umieszczone na różnych zakładkach:

- **Monitorowanie**. Wyświetla w czasie rzeczywistym informacje dotyczące działania aplikacji oraz bieżącego stanu urządzeń klienckich. Informacje ważne dla administratora (takie jak wiadomości dotyczące luk, błędów lub wykrytych wirusów) są oznaczone specjalnym kolorem. Możesz użyć odnośników dostępnych na zakładce **Monitorowanie** do wykonywania standardowych zadań administratora (na przykład, do instalowania i konfigurowania aplikacji antywirusowej na urządzeniach klienckich), a także do przejścia do innych folderów drzewa konsoli.

- **Statystyki**. Zawiera zestaw wykresów pogrupowanych według tematów (stan ochrony, statystyki antywirusowe, aktualizacje itd.). Wykresy przedstawiają bieżące informacje dotyczące działania aplikacji i stanu urządzeń klienckich.

- **Raporty**. Zawiera szablony raportów wygenerowanych przez aplikację. Na tej zakładce można utworzyć raporty przy użyciu predefiniowanych szablonów, a także utworzyć swoje własne szablony raportów.

- Okno **Zdarzenia**. Zawiera wpisy dotyczące zdarzeń zarejestrowanych podczas działania aplikacji. Wpisy są podzielone według tematów w celu ułatwienia ich czytania i filtrowania. Na tej zakładce możesz wyświetlić

wybory zdarzeń wygenerowane automatycznie, a także utworzyć swoje własne wybory.

Foldery w węźle Serwer administracyjny

Węzeł **Serwer administracyjny – <Nazwa urządzenia>** zawiera następujące foldery:

- **Zarządzane urządzenia**. Ten folder jest przeznaczony do przechowywania, wyświetlania, konfiguracji i modyfikacji struktury grup administracyjnych, zasad grupowych i zadań grupowych.
- **Zarządzanie urządzeniami mobilnymi**. W tym folderze można zarządzać urządzeniami mobilnymi. W folderze **Zarządzanie urządzeniami mobilnymi** znajdują się następujące podfoldery:
  - **Serwery urządzeń mobilnych**. Przeznaczony do zarządzania serwerami iOS MDM i serwerami urządzeń mobilnych Microsoft Exchange.
  - **Urządzenia mobilne**. Ten podfolder umożliwia zarządzanie urządzeniami mobilnymi z KES, Exchange ActiveSync i iOS MDM.
  - **Certyfikaty**. W tym miejscu można zarządzać certyfikatami urządzeń mobilnych.
- **Wybory urządzeń**. Ten folder jest przeznaczony do szybkiego wyboru urządzeń, które spełniają określone kryteria (wybór urządzeń), spośród wszystkich zarządzanych urządzeń. Na przykład, możesz szybko wybrać urządzenia, na których nie została zainstalowana żadna aplikacja zabezpieczająca, i przejść do tych urządzeń (wyświetlić listę). Na tych wybranych urządzeniach możesz wykonać pewne działania, na przykład, przypisać do nich zadania. Możesz użyć predefiniowanych wyborów lub utworzyć swoje własne wybory.
- **Urządzenia nieprzypisane**. Ten folder zawiera listę urządzeń, które nie zostały włączone do żadnej grupy administracyjnej. Na nieprzypisanych urządzeniach możesz wykonać różne działania, na przykład, przenieść je do grup administracyjnych lub zainstalować na nich aplikacje.
- **Zasady**. W tym folderze można przeglądać i tworzyć zasady.
- **Zadania**. W tym folderze można przeglądać i tworzyć zadania.
- **Licencje Kaspersky**. Zawiera listę kluczy licencyjnych dostępnych dla aplikacji firmy Kaspersky. W obszarze roboczym tego folderu możesz dodać nowe klucze licencyjne do repozytorium kluczy licencyjnych, rozesłać klucze licencyjne na zarządzane urządzenia, a także wyświetlić raport z użycia kluczy licencyjnych.
- **Zaawansowane**. Ten folder zawiera kilka podfolderów odpowiadających różnym grupom funkcji aplikacji.

Folder Zaawansowane. Przenoszenie folderów w drzewie konsoli

Folder **Zaawansowane** zawiera następujące podfoldery:

- **Konta użytkowników**. Zawiera listę sieciowych kont użytkowników.
- **Zarządzanie aplikacjami**. Przeznaczony do zarządzania aplikacjami zainstalowanymi na urządzeniach w sieci. W folderze **Zarządzanie aplikacjami** znajdują się następujące podfoldery:
  - **Kategorie aplikacji**. Przeznaczony do zarządzania niestandardowymi kategoriami aplikacji.
  - **Rejestr aplikacji**. Zawiera listę aplikacji na urządzeniach, na których zainstalowano Agenta sieciowego.

- **Pliki wykonywalne**. Zawiera listę plików wykonywalnych przechowywanych na urządzeniach klienckich, na których zainstalowano Agenta sieciowego.

- **Luki w oprogramowaniu**. Zawiera listę luk w aplikacjach na urządzeniach, na których zainstalowano Agenta sieciowego.

- **Aktualizacje oprogramowania**. Zawiera listę uaktualnień aplikacji pobranych przez Serwer administracyjny, które mogą zostać przesłane na urządzenia.

- **Wykorzystanie licencji firm trzecich**. Zawiera listę grup licencjonowanych aplikacji. Możesz użyć grup licencjonowanych aplikacji do monitorowania użycia licencji dla oprogramowania firm trzecich (aplikacje, które nie zostały stworzone przez firmę Kaspersky) i możliwych naruszeń ograniczeń licencji.

- **Zdalna instalacja**. Ten folder służy do zarządzania zdalną instalacją systemów operacyjnych i aplikacji. W folderze **Zdalna instalacja** znajdują się następujące podfoldery:

  - **Rozsyłanie obrazów urządzenia**. Służy do instalowania obrazów systemów operacyjnych na urządzeniach.

  - **Pakiety instalacyjne**. Zawiera listę pakietów instalacyjnych, których można użyć do zdalnej instalacji aplikacji na urządzeniach.

- **Szyfrowanie i ochrona danych**. Ten folder służy do zarządzania postępem szyfrowania danych na dyskach i nośnikach wymiennych.

- **Przeszukiwanie sieci**. W tym folderze jest wyświetlana sieć, w której zainstalowany jest Serwer administracyjny. Serwer administracyjny otrzymuje informacje o strukturze sieci i jej urządzeniach poprzez regularne przeszukiwanie sieci Windows, podsieci IP i Active Directory® w sieci korporacyjnej. Wyniki przeszukiwania wyświetlane są w obszarach roboczych odpowiednich folderów: **Domeny**, **Zakresy IP** oraz **Active Directory**.

- **Repozytoria**. Ten folder jest przeznaczony do pracy z obiektami wykorzystywanymi do monitorowania stanu urządzeń klienckich i ich obsługiwania. Folder **Repozytoria** zawiera następujące podfoldery:

  - **Adaptacyjne wykrywanie anomalii**. Zawiera listę elementów wykrytych przez reguły Kaspersky Endpoint Security działające w trybie Inteligentne uczenie na urządzeniach klienckich.

  - **Aktualizacje i poprawki oprogramowania Kaspersky**. Zawiera listę uaktualnień pobranych przez Serwer administracyjny, które mogą zostać przesłane do komputerów klienckich.

  - **Sprzęt**. Zawiera listę sprzętu podłączonego do sieci firmowej.

  - **Kwarantanna**. Zawiera listę obiektów przeniesionych do Kwarantanny przez oprogramowanie antywirusowe znajdujące się na urządzeniach.

  - **Kopia zapasowa**. Zawiera listę kopii zapasowych plików, które w wyniku procesu leczenia zostały usunięte lub zmodyfikowane.

  - **Nieprzetworzone pliki**. Zawiera listę plików przeznaczonych do późniejszego skanowania przez aplikacje antywirusowe.

Możesz zmienić zestaw podfolderów znajdujących się w folderze **Zaawansowane**. Często używane podfoldery można przenieść o jeden poziom wyżej z folderu **Zaawansowane**. Rzadko używane podfoldery można przenieść do folderu **Zaawansowane**.

*W celu przeniesienia podfolderu poza obszar folderu **Zaawansowane**:*

1. W drzewie konsoli wybierz podfolder, który chcesz przenieść poza obszar folderu **Zaawansowane**.

2. W menu kontekstowym podfolderu wybierz **Widok** → **Przenieś z folderu Zaawansowane**.

Podfolder można przenieść poza obszar folderu **Zaawansowane** także z poziomu obszaru roboczego folderu **Zaawansowane**, klikając odnośnik **Przenieś z folderu Zaawansowane** w sekcji z nazwą tego podfolderu.

*W celu przeniesienia podfolderu do folderu **Zaawansowane**:*

1. W drzewie konsoli wybierz podfolder, który chcesz przenieść do folderu **Zaawansowane**.
2. W menu kontekstowym podfolderu wybierz **Widok** → **Przenieś do folderu Zaawansowane**.

Jak zaktualizować dane w obszarze roboczym

W Kaspersky Security Center dane w obszarze roboczym (stany urządzeń, statystyki i raporty) nigdy nie są aktualizowane automatycznie.

W celu zaktualizowania danych w obszarze roboczym:

- Wciśnij klawisz **F5**.
- W menu kontekstowym obiektu z drzewa konsoli wybierz **Odśwież**.
- Kliknij ikonę odśwież () w obszarze roboczym.

Jak poruszać się po drzewie konsoli

Do poruszania się po drzewie konsoli możesz użyć następujących przycisków paska narzędzi:

-  – jeden krok wstecz.
-  – jeden krok do przodu.
-  – jeden poziom wyżej.

Możesz także użyć łańcucha nawigacji znajdującego się w prawym górnym rogu obszaru roboczego. Panel nawigacyjny zawiera pełną ścieżkę do foldera drzewa konsoli, w którym się znajdujesz. Wszystkie elementy panelu (za wyjątkiem ostatniego) są odnośnikami do obiektów w drzewie konsoli.

Jak w obszarze roboczym otworzyć okno właściwości obiektu

Właściwości większości obiektów Konsoli administracyjnej możesz zmienić w oknie właściwości obiektu.

W celu otwarcia okna właściwości obiektu znajdującego się w obszarze roboczym:

- Z menu kontekstowego obiektu wybierz **Właściwości**.

- Zaznacz obiekt i wciśnij **ALT**+**ENTER**.

Jak w obszarze roboczym wybrać grupę obiektów

Grupę obiektów możesz wybrać w obszarze roboczym. Możesz wybrać grupę obiektów, na przykład, do utworzenia zbioru urządzeń, dla których możesz utworzyć zadania w późniejszym czasie.

W celu wybrania zakresu obiektów:

1. Wybierz pierwszy obiekt z zakresu i wciśnij **Shift**.
2. Przytrzymaj wciśnięty klawisz **Shift** i wybierz ostatni obiekt z zakresu.

   Zakres zostanie wybrany.

W celu pogrupowania oddzielnych obiektów:

1. Wybierz pierwszy obiekt z grupy i wciśnij **Ctrl**.
2. Przytrzymaj wciśnięty klawisz **Ctrl** i wybierz inne obiekty, które chcesz uwzględnić w grupie.

   Obiekty zostaną pogrupowane.

Jak zmienić zestaw kolumn w obszarze roboczym

Konsola administracyjna umożliwia zmianę zestawu kolumn wyświetlanych w obszarze roboczym.

W celu zmiany zestawu kolumn wyświetlanych w obszarze roboczym:

1. W drzewie konsoli kliknij obiekt, dla którego chcesz zmienić zestaw kolumn.
2. W obszarze roboczym folderu otwórz okno przeznaczone do konfigurowania zestawu kolumn, klikając odnośnik **Dodaj/Usuń kolumny**.
3. W oknie **Dodaj/Usuń kolumny** określ zestaw wyświetlanych kolumn.

Informacje dodatkowe

Tabele w tej sekcji zawierają informacje o menu kontekstowym obiektów Konsoli administracyjnej oraz o stanach obiektów drzewa konsoli i obiektów obszaru roboczego.

Polecenia menu kontekstowego

Ta sekcja wyświetla obiekty Konsoli administracyjnej i odpowiadające im elementy menu kontekstowego (patrz tabela poniżej).

Obiekt	Element menu	Przeznaczenie elementu menu
Ogólne elementy menu kontekstowego	**Szukaj**	Otwiera okno wyszukiwania urządzeń.
	Odśwież	Odświeża wyświetlanie wybranego obiektu.
	Eksportuj listę	Eksportuje bieżącą listę do pliku.
	Właściwości	Otwiera okno właściwości wybranego obiektu.
	Widok → Dodaj/Usuń kolumny	Dodaje lub usuwa kolumny w tabeli obiektów, w obszarze roboczym.
	Widok → Duże ikony	Wyświetla obiekty w obszarze roboczym jako duże ikony.
	Widok → Małe ikony	Wyświetla obiekty w obszarze roboczym jako małe ikony.
	Widok → Lista	Wyświetla obiekty w obszarze roboczym w postaci listy.
	Widok → Tabela	Wyświetla obiekty w obszarze roboczym w postaci tabeli.
	Widok → Konfiguruj	Konfiguruje wyświetlanie elementów Konsoli administracyjnej.
Kaspersky Security Center	**Nowa → Serwer administracyjny**	Dodaje Serwer administracyjny do drzewa konsoli.
<Nazwa Serwera administracyjnego>	**Połącz z Serwerem administracyjnym**	Nawiązuje połączenie z Serwerem administracyjnym.
	Odłącz od Serwera administracyjnego	Odłącza od Serwera administracyjnego
Zarządzane urządzenia	**Zainstaluj aplikację**	Uruchamia Kreator zdalnej instalacji.
	Widok → Konfiguruj interfejs	Konfiguruje wyświetlanie elementów interfejsu.
	Usuń	Usuwa Serwer administracyjny z drzewa konsoli.
	Zainstaluj aplikację	Uruchamia Kreator zdalnej instalacji dla grupy administracyjnej.
	Resetuj licznik wirusów	Resetuje licznik wirusów dla urządzeń znajdujących się w grupie administracyjnej.
	Wyświetl raport o zagrożeniach	Tworzy raport o zagrożeniach i aktywności wirusów na urządzeniach znajdujących się w grupie administracyjnej.
	Nowy → Grupa	Tworzy grupę administracyjną.
	Wszystkie zadania → Nowa struktura grupy	Tworzy strukturę grup administracyjnych w oparciu o strukturę domen lub Active Directory.
	Wszystkie zadania → Pokaż wiadomość	Uruchamia Kreator tworzenia nowej wiadomości dla użytkownika, przeznaczony dla użytkowników urządzeń należących do grupy administracyjnej.
Zarządzane urządzenia → Serwery administracyjne	**Nowy → Podrzędny Serwer administracyjny**	Uruchamia Kreator dodawania podrzędnego Serwera administracyjnego.

	Nowy → Wirtualny Serwer administracyjny	Uruchamia Kreator tworzenia nowego wirtualnego Serwera administracyjnego.
Zarządzanie urządzeniami mobilnymi → Urządzenia mobilne	**Nowa → Urządzenie mobilne**	Podłącza nowe urządzenie mobilne użytkownika.
Zarządzanie urządzeniami mobilnymi → Certyfikaty	**Nowy → Certyfikat**	Tworzy certyfikat.
	Utwórz → Urządzenie mobilne	Podłącza nowe urządzenie mobilne użytkownika.
Wybory urządzeń	**Nowy → Nowy wybór**	Tworzy wybór urządzeń.
	Wszystkie zadania → Importuj	Importuje wybór z pliku.
Licencje Kaspersky	**Dodaj kod aktywacyjny lub plik klucza**	Dodaje klucz licencyjny do repozytorium Serwera administracyjnego.
	Aktywuj aplikację	Uruchamia Kreator tworzenia zadania aktywacji aplikacji.
	Raport o użyciu kluczy licencyjnych	Tworzy i wyświetla raport o kluczach licencyjnych na urządzeniach klienckich.
Zarządzanie aplikacjami → Kategorie aplikacji	**Nowy → Kategoria**	Tworzy kategorię aplikacji.
Zarządzanie aplikacjami → Rejestr aplikacji	**Filtr**	Konfiguruje filtr dla listy aplikacji.
	Monitorowane aplikacje	Konfiguruje publikowanie zdarzeń związanych z instalacją aplikacji.
	Usuń aplikacje, które nie są zainstalowane	Tworzy listę wszystkich szczegółów aplikacji, które nie są już zainstalowane na urządzeniach w sieci.
Zarządzanie aplikacjami → Aktualizacje oprogramowania	**Akceptuj warunki Umów licencyjnych aktualizacji**	Akceptuje Umowy licencyjne dla uaktualnień oprogramowania.
Zarządzanie aplikacjami → Wykorzystanie licencji firm trzecich	**Nowy → Grupa licencjonowanych aplikacji**	Tworzy grupę licencjonowanych aplikacji.
Zdalna instalacja → Pakiety instalacyjne	**Pokaż aktualne wersje aplikacji**	Wyświetla listę aktualnych wersji aplikacji Kaspersky dostępnych na serwerach sieciowych.
	Nowy → Pakiet instalacyjny	Tworzy pakiet instalacyjny.
	Wszystkie zadania → Aktualizuj bazy danych	Aktualizuje bazy danych aplikacji w pakietach instalacyjnych.
	Wszystkie zadania → Pokaż ogólną listę pakietów autonomicznych	Wyświetla listę autonomicznych pakietów utworzonych dla pakietów instalacyjnych.
Wykrywanie urządzeń → Domeny	**Wszystkie zadania → Aktywność urządzenia**	Ustawia odpowiedź Serwera administracyjnego na brak aktywności urządzeń w sieci.
Wykrywanie urządzeń → Zakresy IP	**Nowy → Zakres IP**	Tworzy zakres IP.

Repozytoria → Aktualizacje baz danych i modułów oprogramowania Kaspersky	**Pobierz uaktualnienia**	Otwiera okno właściwości zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego.
	Ustawienia pobierania aktualizacji	Konfiguruje zadanie Pobierz uaktualnienia do repozytorium Serwera administracyjnego.
	Raport o używanych antywirusowych bazach danych	Tworzy i wyświetla raport o wersjach baz danych.
	Wszystkie zadania → Wyczyść repozytorium uaktualnień	Czyści repozytoria aktualizacji na Serwerze administracyjnym.
Repozytoria → Sprzęt	**Nowy → Urządzenie**	Tworzy nowe urządzenie.

Lista zarządzanych urządzeń. Opis kolumn

Poniższa tabela wyświetla nazwy i odpowiednie opisy kolumn listy zarządzanych urządzeń.

Opisy kolumn listy zarządzanych urządzeń

Nazwa kolumny	Wartość
Nazwa	Nazwa NetBIOS urządzenia klienckiego. Opisy ikon nazw urządzeń są podane w dodatku.
Typ systemu operacyjnego	Typ systemu operacyjnego zainstalowanego na urządzeniu klienckim.
Domena Windows	Nazwa domeny Windows, w której znajduje się urządzenie klienckie.
Agent sieciowy jest zainstalowany	Wynik instalacji Agenta sieciowego na urządzeniu klienckim (*Tak*, *Nie*, *Nieznany*).
Agent sieciowy jest uruchomiony	Wynik działania Agenta sieciowego (*Tak*, *Nie*, *Nieznany*).
Ochrona w czasie rzeczywistym	Aplikacja zabezpieczająca jest zainstalowana (*Tak*, *Nie*, *Nieznany*).
Ostatnie połączenie z Serwerem administracyjnym	Czas, jaki upłynął od momentu połączenia urządzenia klienckiego z Serwerem administracyjnym.
Ostatnia aktualizacja ochrony	Okres, który upłynął od ostatniej aktualizacji zarządzanych urządzeń.
Stan	Bieżący stan urządzenia klienckiego (*OK, Krytyczny lub Ostrzeżenie)*.
Opis stanu	Przyczyna zmiany stanu urządzenia klienckiego na *Krytyczny* lub *Ostrzeżenie*. Stan urządzenia zmienia się na *Ostrzeżenie* lub *Krytyczny* z następujących powodów: • Aplikacja zabezpieczająca nie jest zainstalowana. • Wykryto zbyt wiele wirusów.

	• Poziom ochrony w czasie rzeczywistym jest inny niż poziom zdefiniowany przez administratora. • Skanowanie w poszukiwaniu złośliwego oprogramowania nie było wykonywane od dłuższego czasu • Bazy danych są nieaktualne. • Niepołączony od dłuższego czasu. • Wykryto aktywne zagrożenia. • Wymagane jest ponowne uruchomienie. • Zainstalowane są niekompatybilne aplikacje. • Wykryto luki w oprogramowaniu. • Wyszukiwanie aktualizacji Windows Update nie było przeprowadzane od dłuższego czasu. • Nieprawidłowy stan szyfrowania. • Ustawienia urządzenia mobilnego nie są zgodne z zasadą. • Wykryto nieprzetworzone incydenty. • Stan urządzenia zdefiniowany przez aplikację. • Brakuje miejsca na dysku urządzenia. • Licencja wkrótce utraci ważność. Stan urządzenia zmienia się tylko na *Krytyczny* z następujących powodów: • Licencja utraciła ważność. • Zarządzanie urządzeniem nie jest możliwe. • Ochrona jest wyłączona. • Aplikacja zabezpieczająca nie jest uruchomiona. Zarządzane aplikacje Kaspersky na urządzeniach klienckich mogą dodawać opisy stanów do listy. Kaspersky Security Center może pobrać opis stanu urządzenia klienckiego od zarządzanych aplikacji Kaspersky, zainstalowanych na tym urządzeniu. Jeśli stan, który został przypisany do urządzenia przez zarządzaną aplikację, różni się od stanu przypisanego przez Kaspersky Security Center, Konsola administracyjna wyświetla stan, który jest najbardziej krytyczny dla bezpieczeństwa urządzenia. Na przykład, jeśli zarządzana aplikacja przypisała do urządzenia stan *Krytyczny*, a Kaspersky Security Center przypisał do niego stan *Ostrzeżenie*, Konsola administracyjna wyświetli dla tego urządzenia stan *Krytyczny* oraz odpowiedni opis dostarczony przez zarządzaną aplikację.
Ostatnia aktualizacja informacji	Czas, jaki upłynął od momentu ostatniej pomyślnej synchronizacji urządzenia klienckiego z Serwerem administracyjnym (czyli od ostatniego skanowania sieci).

Nazwa DNS	Nazwa domeny DNS urządzenia klienckiego.
Domena DNS	Główny sufiks DNS.
Adres IP	Adres IP urządzenia klienckiego. Zalecane jest użycie adresu IPv4.
Ostatnio dostępny	Okres, przez jaki urządzenie klienckie było widoczne w sieci.
Ostatnie pełne skanowanie	Data i godzina ostatniego skanowania urządzenia klienckiego, które zostało wykonane przez aplikację antywirusową na żądanie użytkownika.
Łączna liczba wykrytych zagrożeń	Liczba wykrytych zagrożeń.
Stan ochrony w czasie rzeczywistym	Stan ochrony w czasie rzeczywistym (*Uruchamianie, Uruchomiona, Uruchomiona (maksymalna ochrona), Uruchomiona (wysoka wydajność), Uruchomiona (ustawienia zalecane), Uruchomiona (ustawienia niestandardowe), Zatrzymana, Wstrzymana, Niepowodzenie*).
Adres IP połączenia	Adres IP używany do łączenia z Serwerem administracyjnym Kaspersky Security Center.
Wersja Agenta sieciowego	Wersja Agenta sieciowego.
Wersja aplikacji	Wersja aplikacji zabezpieczającej zainstalowanej na urządzeniu klienckim.
Ostatnia aktualizacja antywirusowych baz danych	Wersja antywirusowych baz danych.
Ostatnie uruchomienie systemu	Data i godzina, kiedy urządzenie klienckie było ostatnio włączane.
Wymagane jest ponowne uruchomienie	Wymagane jest ponowne uruchomienie urządzenia.
Punkt dystrybucji	Nazwa urządzenia, które pełni rolę punktu dystrybucji dla tego urządzenia klienckiego.
Opis	Opis urządzenia klienckiego otrzymany po przeskanowaniu sieci.
Stan szyfrowania	Stan szyfrowania danych urządzenia klienckiego.
Stan WUA	Stan agenta usługi Windows Update na urządzeniu klienckim. *Tak* odnosi się do urządzeń klienckich, które pobrały aktualizacje poprzez usługę Windows Update z Serwera administracyjnego. *Nie* odnosi się do urządzeń klienckich, które pobrały aktualizacje poprzez usługę Windows Update z innych źródeł.
Typ systemu operacyjnego (bity)	Ilość bitów systemu operacyjnego zainstalowanego na urządzeniu klienckim.
Stan ochrony antyspamowej	Stan ochrony przed spamem (*Uruchomione, Uruchamianie, Zatrzymana, Wstrzymano, Niepowodzenie, Brak danych z urządzenia)*
Stan ochrony przed wyciekiem danych	Stan ochrony przed wyciekiem danych (*Uruchomione, Uruchamianie, Zatrzymana, Wstrzymano, Niepowodzenie, Brak danych z urządzenia)*
Stan ochrony	Stan filtrowania zawartości (*Uruchomione, Uruchamianie, Zatrzymana, Wstrzymano,*

serwerów współpracy	*Niepowodzenie, Brak danych z urządzenia)*
Stan ochrony antywirusowej serwerów pocztowych	Stan ochrony antywirusowej serwera pocztowego (*Uruchomione, Uruchamianie, Zatrzymana, Wstrzymano, Niepowodzenie, Brak danych z urządzenia)*
Stan czujnika Endpoint Sensor	Stan komponentu Endpoint Sensor (*Uruchomione, Uruchamianie, Zatrzymana, Wstrzymano, Niepowodzenie, Brak danych z urządzenia)*
Utworzone	Godzina utworzenia ikony <Nazwa urządzenia>. Ten atrybut jest używany do porównywania różnych zdarzeń.
Nazwa wirtualnego lub podrzędnego Serwera administracyjnego	Nazwa wirtualnego lub podrzędnego Serwera administracyjnego Ta kolumna jest dostępna tylko na listach, które zawierają urządzenia z różnych Serwerów administracyjnych.
Grupa nadrzędna	Nazwa grupy administracyjnej, w której znajduje się ikona <Nazwa urządzenia>. Ta kolumna jest dostępna tylko na listach, które zawierają urządzenia z różnych Serwerów administracyjnych.
Zarządzane przez inny Serwer administracyjny	Parametr może przyjąć jedną z tych wartości: • True, jeśli podczas zdalnej instalacji aplikacji zabezpieczających na urządzeniu okaże się, że urządzenie jest zarządzane przez inny Serwer administracyjny. • False - w innym przypadku.
Kompilacja systemu operacyjnego	Numer kompilacji systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować wyszukiwanie wszystkich numerów kompilacji, za wyjątkiem określonego.
ID wersji systemu operacyjnego	Identyfikator wydania systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy identyfikator wydania. Możesz także skonfigurować wyszukiwanie wszystkich numerów identyfikatorów wydania, za wyjątkiem określonego.

Stany przypisane do urządzeń, zadań i profili

Poniższa tabela zawiera listę ikon wyświetlanych w drzewie konsoli i obszarze roboczym Konsoli administracyjnej obok nazw urządzeń, zadań i profili. Ikony te przedstawiają stany obiektów.

Stany przypisane do urządzeń, zadań i profili

Ikona	Stan
	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, wykryte w systemie, ale nie znajdujące się w żadnej grupie administracyjnej.

	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, należące do grupy administracyjnej, ze stanem *OK*.
	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, należące do grupy administracyjnej, ze stanem *Ostrzeżenie*.
	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, należące do grupy administracyjnej, ze stanem *Krytyczny*.
	Urządzenie z zainstalowanym systemem operacyjnym dla stacji roboczych, należące do grupy administracyjnej; jego połączenie z Serwerem administracyjnym zostało zerwane.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, wykryte w systemie, ale nie znajdujące się w żadnej grupie administracyjnej.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, należące do grupy administracyjnej, ze stanem *OK*.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, należące do grupy administracyjnej, ze stanem *Ostrzeżenie*.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, należące do grupy administracyjnej, ze stanem *Krytyczny*.
	Urządzenie z zainstalowanym systemem operacyjnym dla serwerów, należące do grupy administracyjnej; jego połączenie z Serwerem administracyjnym zostało zerwane.
	Urządzenie mobilne wykryte w sieci i nie uwzględnione w żadnej grupie administracyjnej.
	Urządzenie mobilne, znajdujące się w grupie administracyjnej, ze stanem *OK*.
	Urządzenie mobilne, znajdujące się w grupie administracyjnej, ze stanem *Ostrzeżenie*.
	Urządzenie mobilne, znajdujące się w grupie administracyjnej, ze stanem *Krytyczny*.
	Urządzenie mobilne należące do grupy administracyjnej, jego połączenie z Serwerem administracyjnym zostało zerwane.
	Urządzenie chronione UEFI wykryte w sieci, ale nie należące do żadnej grupy administracyjnej. Urządzenie chronione UEFI znajduje się w sieci.
	Urządzenie chronione UEFI wykryte w sieci, ale nie należące do żadnej grupy administracyjnej. Urządzenie chronione UEFI nie znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *OK*. Urządzenie chronione UEFI znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *OK*. Urządzenie chronione UEFI nie znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *Ostrzeżenie*. Urządzenie chronione UEFI znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *Ostrzeżenie*. Urządzenie chronione UEFI nie znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *Krytyczny*. Urządzenie chronione UEFI znajduje się w sieci.
	Urządzenie chronione UEFI, znajdujące się w grupie administracyjnej, ze stanem *Krytyczny*. Urządzenie chronione UEFI nie znajduje się w sieci.
	Profil aktywny.
	Profil nieaktywny.

	Zasada aktywna dziedziczona od grupy, która została utworzona na głównym Serwerze administracyjnym.
	Profil aktywny dziedziczony od grupy z wyższego poziomu hierarchii.
	Zadanie (grupowe, Serwera administracyjnego lub dla wskazanych urządzeń) ze stanem *Zaplanowane* lub *Pomyślnie zakończone*.
	Zadanie (grupowe, Serwera administracyjnego lub dla wskazanych urządzeń) ze stanem *Uruchomione*.
	Zadanie (grupowe, Serwera administracyjnego lub dla wskazanych urządzeń) ze stanem *Niepowodzenie*.
	Zadanie dziedziczone od grupy, która została utworzona na głównym Serwerze administracyjnym.
	Zadanie dziedziczone od grupy z wyższego poziomu hierarchii.

Ikony stanów plików w Konsoli administracyjnej

Aby ułatwić zarządzanie plikami w Konsoli administracyjnej Kaspersky Security Center, obok nazw plików wyświetlane są ikony (patrz tabela poniżej). Ikony wskazują stany przypisane do plików przez zarządzane aplikacje Kaspersky na urządzeniach klienckich. Ikony są wyświetlane w obszarach roboczych folderów **Kwarantanna**, **Kopia zapasowa** i **Aktywne zagrożenia**.

Stany są przydzielane do obiektów przez program Kaspersky Endpoint Security zainstalowany na urządzeniu klienckim, na którym znajduje się obiekt.

Zgodność ikon ze stanami plików

Ikona	Stan
	Plik ze stanem *Zainfekowany*.
	Plik ze stanem *Ostrzeżenie* lub *Prawdopodobnie zainfekowany*.
	Plik ze stanem *Dodany przez użytkownika*.
	Plik ze stanem *Fałszywy alarm*.
	Plik ze stanem *Wyleczony*.
	Plik ze stanem *Usunięty*.
	Plik w folderze **Kwarantanna** ze stanem *Niezainfekowany, Zabezpieczony hasłem* lub *Musi zostać przesłany do firmy Kaspersky*. Jeśli obok ikony nie ma opisu stanu, oznacza to, że zarządzana aplikacja firmy Kaspersky na urządzeniu klienckim zgłosiła stan nieznany Kaspersky Security Center.
	Plik w folderze **Kopia zapasowa** ze stanem *Niezainfekowany, Zabezpieczony hasłem* lub *Musi zostać przesłany do firmy Kaspersky*. Jeśli obok ikony nie ma opisu stanu, oznacza to, że zarządzana aplikacja firmy Kaspersky na urządzeniu klienckim zgłosiła stan nieznany Kaspersky Security Center.
	Plik w folderze **Aktywne zagrożenia** ze stanem *Niezainfekowany, Zabezpieczony hasłem* lub *Musi zostać przesłany do firmy Kaspersky*. Jeśli obok ikony nie ma opisu stanu, oznacza to, że zarządzana aplikacja firmy Kaspersky na urządzeniu klienckim zgłosiła stan nieznany Kaspersky Security Center.

Wyszukiwanie i eksportowanie danych

Ta sekcja zawiera informacje o metodach wyszukiwania danych oraz o eksportowaniu danych.

Wyszukiwanie urządzeń

Kaspersky Security Center umożliwia wyszukiwanie urządzeń w oparciu o określone kryteria. Wyniki wyszukiwania można zapisać do pliku tekstowego.

Opcja wyszukiwania pozwala znaleźć następujące urządzenia:

- Urządzenia klienckie w grupach administracyjnych Serwera administracyjnego i jego Serwerów podrzędnych.
- Nieprzypisane urządzenia zarządzane przez Serwer administracyjny i jego Serwery podrzędne.

W celu wyszukania urządzeń klienckich znajdujących się w grupie administracyjnej:

1. W drzewie konsoli wybierz folder grupy administracyjnej.
2. Wybierz **Szukaj** z menu kontekstowego folderu grupy administracyjnej.
3. Na zakładkach w oknie **Szukaj** określ kryteria wyszukiwania urządzeń, a następnie kliknij przycisk **Znajdź teraz**.

   Urządzenia, które spełniają określone kryteria wyszukiwania, są teraz wyświetlane w tabeli, w dolnej części okna **Szukaj**.

W celu wyszukania urządzeń nieprzypisanych:

1. Z drzewa konsoli wybierz folder **Urządzenia nieprzypisane**.
2. Wybierz **Szukaj** z menu kontekstowego folderu **Urządzenia nieprzypisane**.
3. Na zakładkach w oknie **Szukaj** określ kryteria wyszukiwania urządzeń, a następnie kliknij przycisk **Znajdź teraz**.

   Urządzenia, które spełniają określone kryteria wyszukiwania, są teraz wyświetlane w tabeli, w dolnej części okna **Szukaj**.

W celu wyszukania urządzeń niezależnie od tego, czy znajdują się w grupie administracyjnej:

1. W drzewie konsoli wybierz węzeł **Serwer administracyjny** .
2. Z otwartego menu kontekstowego węzła wybierz **Szukaj**.
3. Na zakładkach w oknie **Szukaj** określ kryteria wyszukiwania urządzeń, a następnie kliknij przycisk **Znajdź teraz**.

   Urządzenia, które spełniają określone kryteria wyszukiwania, są teraz wyświetlane w tabeli, w dolnej części okna **Szukaj**.

W oknie **Szukaj** możesz także wyszukać grupy administracyjne i podrzędne Serwery administracyjne, korzystając z listy rozwijalnej dostępnej w prawym górnym rogu okna. Funkcjonalność wyszukiwania grup administracyjnych i podrzędnych Serwerów administracyjnych nie jest dostępna, jeśli okno **Szukaj** zostało otwarte z poziomu folderu **Urządzenia nieprzypisane**.

Aby wyszukać urządzenia, w oknie **Szukaj** możesz użyć wyrażeń regularnych.

Wyszukiwanie pełnotekstowe jest dostępne w oknie **Szukaj**:

- Na zakładce **Sieć**, w polu **Opis**
- Na zakładce **Sprzęt**, w polach **Urządzenie**, **Producent** i **Opis**

Ustawienia wyszukiwania urządzeń

Poniżej znajdują się opisy ustawień używanych do wyszukiwania zarządzanych urządzeń. Wyniki wyszukiwania są wyświetlane w dolnej części okna.

Sieć

Na zakładce **Sieć** możesz określić kryteria, które będą używane do wyszukiwania urządzeń według ich danych sieciowych:

- **Nazwa urządzenia lub adres IP**

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- **Domena Windows**

  Wyświetla wszystkie urządzenia znajdujące się w określonej domenie Windows.

- **Grupa administracyjna**

  Wyświetla urządzenia znajdujące się w określonej grupie administracyjnej.

- **Opis**

Tekst wyświetlany w oknie właściwości urządzenia: pole **Opis** sekcji **Ogólny**.

W celu opisania tekstu w polu **Opis** możesz użyć następujących znaków:

- W słowie:
  - *****. Zastępuje dowolny wiersz dowolną liczbą znaków.

    Na przykład:

    Aby opisać słowa **Serwer** lub **Serwera**, możesz wpisać **Serwer***.
  - **?.** Zastępuje dowolny pojedynczy znak.

    Na przykład:

    Aby opisać słowa **Okno** lub **Okna**, możesz wpisać **Okn?**.

    Gwiazdka (*****) lub znak zapytania (**?**) nie mogą być używane jako pierwsze symbole wyszukiwanego słowa.
- W celu wyszukania kilku słów użyj:
  - Spacji. Wyświetla wszystkie urządzenia, których opisy zawierają dowolne z wymienionych słów.

    Na przykład:

    Aby odszukać frazę zawierającą słowa **Podrzędny** lub **Wirtualny**, wprowadź **Podrzędny Wirtualny** w tekście wyszukiwania.
  - **+**. Jeśli przed wyrazem wpisano znak "+", wszystkie wyniki wyszukiwania będą zawierać ten wyraz.

    Na przykład:

    Aby odszukać frazę zawierającą zarówno **Podrzędny**, jak i **Wirtualny**, wprowadź **+Podrzędny+Wirtualny**.
  - **-**. Jeśli przed wyrazem wpisano znak "-", żaden z wyników wyszukiwania nie będzie zawierać tego wyrazu.

    Na przykład:

    Aby odszukać frazę zawierającą **Podrzędny** i nie zawierającą **Wirtualny**, wprowadź **+Podrzędny-Wirtualny**.
  - **"<jakikolwiek tekst>"**. Tekst w cudzysłowach musi znajdować się w tekście.

    Na przykład:

    Aby odszukać frazę zawierającą kombinację słów **Podrzędny Serwer**, wprowadź **„Podrzędny Serwer"** w tekście wyszukiwania.

- Zakres IP

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

- Zarządzane przez inny Serwer administracyjny

Wybierz jedną z następujących wartości:

- **Tak**. Brane pod uwagę są tylko urządzenia klienckie zarządzane przez inne Serwery administracyjne.
- **Nie**. Brane pod uwagę są tylko urządzenia klienckie zarządzane przez ten sam Serwer administracyjny.
- **Nie wybrano wartości**. Kryterium nie będzie stosowane.

Znaczniki

Na zakładce **Znaczniki** możesz skonfigurować wyszukiwanie urządzeń w oparciu o słowa kluczowe (znaczniki), które wcześniej zostały dodane do opisów zarządzanych urządzeń:

- Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny

  Jeśli ta opcja jest włączona, w wynikach wyszukiwania będą wyświetlane urządzenia z opisami, które zawierają przynajmniej jeden z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, w wynikach wyszukiwania będą wyświetlane tylko urządzeni z opisami, które zawierają wszystkie wybrane znaczniki.

  Domyślnie opcja ta jest wyłączona.

- Musi zawierać znacznik

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy zawierają wybrany znacznik. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

  Domyślnie opcja ta jest zaznaczona.

- Nie może zawierać znacznika

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy nie zawierają wybranego znacznika. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

Active Directory

Na zakładce **Active Directory** można określić, że urządzenia mają być wyszukiwane w jednostce organizacyjnej (OU) lub grupie Active Directory. W wyborze można również uwzględnić urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej Active Directory. W celu wybrania urządzeń, zdefiniuj następujące ustawienia:

- Urządzenie znajduje się w jednostce organizacyjnej Active Directory

  Jeśli ta opcja jest włączona, wybór będzie zawierał urządzenia z jednostki Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

- Uwzględnij podrzędne jednostki organizacyjne

Jeśli ta opcja jest włączona, wybór zawiera urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej Active Directory.

Domyślnie opcja ta jest wyłączona.

- Urządzenie należy do grupy Active Directory

  Jeśli ta opcja jest włączona, wybór będzie zawierał komputery z grupy Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

Aktywność sieciowa

Na zakładce **Aktywność sieciowa** możesz określić kryteria, które będą używane do wyszukiwania urządzeń według ich aktywności sieciowej:

- Urządzenie jest punktem dystrybucji

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:
  - **Tak**. Wybór zawiera urządzenia pełniące role punktów dystrybucji.
  - **Nie**. Urządzenia pełniące role punktów dystrybucji nie będą uwzględniane w wyborze.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Nie odłączaj od Serwera administracyjnego

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:
  - **Włączono**. Wybór będzie zawierał urządzenia, na których zaznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Wyłączono**. Wybór będzie zawierał urządzenia, na których odznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Przełączanie profilu połączenia

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:
  - **Tak**. Wybór będzie zawierał urządzenia, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie**. Wybór nie będzie zawierał urządzeń, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Ostatnie połączenie z Serwerem administracyjnym

To pole ustawia kryterium wyszukiwania urządzeń według godziny ostatniego połączenia z Serwerem administracyjnym.

Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego zostało nawiązane ostatnie połączenie pomiędzy Agentem sieciowym zainstalowanym na urządzeniu klienckim a Serwerem administracyjnym. Wybór będzie zawierał urządzenia mieszczące się w określonym przedziale czasu.

Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

Domyślnie pole to nie jest zaznaczone.

- Nowe urządzenia odnalezione podczas skanowania sieci

  Wyszukiwanie nowych urządzeń, które zostały wykryte podczas przeszukiwania sieci w przeciągu kilku ostatnich dni.

  Jeśli ta opcja jest włączona, wybór będzie zawierał nowe urządzenia wykryte podczas wykrywania urządzeń w czasie określonym w polu **Okres wykrywania (dni)**.

  Jeśli ta opcja jest wyłączona, wybór będzie zawierał wszystkie urządzenia wykryte podczas wykrywania urządzeń.

  Domyślnie opcja ta jest wyłączona.

- Dostępność urządzenia

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie widoczne w sieci.
  - **Nie**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie niewidoczne w sieci.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

Aplikacja

Na zakładce **Aplikacja** możesz określić kryteria, które będą używane do wyszukiwania urządzeń według wybranej zarządzanej aplikacji:

- Nazwa aplikacji

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji Kaspersky.

  Lista zawiera tylko nazwy aplikacji z wtyczkami administracyjnymi zainstalowanych na stacji roboczej administratora.

  Jeśli żadna aplikacja nie została wybrana, kryterium nie będzie stosowane.

- Wersja aplikacji

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według numeru wersji aplikacji Kaspersky.

  Jeśli żaden numer wersji nie został określony, kryterium nie będzie stosowane.

- Nazwa aktualizacji krytycznej

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji lub numeru pakietu aktualizacyjnego.

  Jeśli pole będzie puste, kryterium nie będzie stosowane.

- Ostatnia aktualizacja modułów

  Ta opcja może zostać użyta do ustawienia kryterium wyszukiwania urządzeń według godziny ostatniej aktualizacji modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego została wykonana ostatnia aktualizacja modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- Urządzenie jest zarządzane przez Kaspersky Security Center

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić urządzenia zarządzane poprzez Kaspersky Security Center:

  - **Tak**. Aplikacja uwzględni w wyborze urządzenia zarządzane poprzez Kaspersky Security Center.
  - **Nie**. Aplikacja uwzględni w wyborze urządzenia, jeśli nie są one zarządzane przez Kaspersky Security Center.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Aplikacja zabezpieczająca jest zainstalowana

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą:

  - **Tak**. Aplikacja uwzględni w wyborze wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą.
  - **Nie**. Aplikacja uwzględni w wyborze wszystkie urządzenia bez zainstalowanej aplikacji zabezpieczającej.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

System operacyjny

Na zakładce **System operacyjny** możesz określić następujące kryteria wyszukiwania urządzeń według typu systemu operacyjnego:

- Wersja systemu operacyjnego

  Jeśli pole jest zaznaczone, możesz wybrać system operacyjny z listy. Urządzenia, na których zainstalowany jest określony system operacyjny, są uwzględniane w wynikach wyszukiwania.

- Typ systemu operacyjnego (bity)

  Z listy rozwijalnej możesz wybrać architekturę swojego systemu operacyjnego, która określi sposób stosowania reguły przenoszenia do urządzenia (**Nieznany**, **x86**, **AMD64**, or **IA64**). Domyślnie, na liście nie wybrano żadnej opcji i tym samym nie zdefiniowano architektury systemu operacyjnego.

- Wersja dodatku Service Pack systemu operacyjnego

  W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- Kompilacja systemu operacyjnego

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Numer kompilacji systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować wyszukiwanie wszystkich numerów kompilacji, za wyjątkiem określonego.

- ID wersji systemu operacyjnego

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Identyfikator wydania systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy identyfikator wydania. Możesz także skonfigurować wyszukiwanie wszystkich numerów identyfikatorów wydania, za wyjątkiem określonego.

Stan urządzenia

Na zakładce **Stan urządzenia** możesz określić kryteria wyszukiwania urządzeń w oparciu o stan urządzenia z zarządzanej aplikacji:

- Stan urządzenia

  Lista rozwijalna, z której możesz wybrać jeden ze stanów urządzenia: *OK*, *Krytyczny*, or *Ostrzeżenie*.

- Stan ochrony w czasie rzeczywistym

  Lista rozwijalna, z której możesz wybrać stan ochrony w czasie rzeczywistym. Urządzenia z określonymi stanami ochrony w czasie rzeczywistym są uwzględniane w wyborze.

- Opis stanu urządzenia

W tym polu możesz zaznaczyć pola obok warunków, które, jeśli są spełnione, spowodują przypisanie do urządzenia jednego z następujących stanów: *OK, Krytyczny*, or *Ostrzeżenie*.

- **Stan urządzenia zdefiniowany przez aplikację**

  Lista rozwijalna, z której możesz wybrać stan ochrony w czasie rzeczywistym. Urządzenia z określonymi stanami ochrony w czasie rzeczywistym są uwzględniane w wyborze.

Składniki ochrony

Na zakładce **Składniki ochrony** możesz skonfigurować kryteria wyszukiwania urządzeń klienckich według stanu ochrony.

- **Data opublikowania baz danych**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według daty opublikowania antywirusowej bazy danych. W polach do wprowadzania danych możesz określić przedział czasu, na podstawie którego wykonywane jest wyszukiwanie.

  Domyślnie opcja ta jest wyłączona.

- **Ostatnie skanowanie**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według czasu ostatniego skanowania w poszukiwaniu złośliwego oprogramowania. W polach wejściowych możesz określić przedział czasu, w trakcie którego zostało wykonane ostatnie skanowanie w poszukiwaniu złośliwego oprogramowania.

  Domyślnie opcja ta jest wyłączona.

- **Łączna liczba wykrytych zagrożeń**

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wykrytych wirusów. W polach wejściowych możesz określić niższe i wyższe wartości progowe liczby wykrytych wirusów.

  Domyślnie opcja ta jest wyłączona.

Rejestr aplikacji

Na zakładce **Rejestr aplikacji** możesz skonfigurować wyszukiwanie urządzeń na podstawie aplikacji na nich zainstalowanych:

- **Nazwa aplikacji**

  Lista rozwijalna, z której możesz wybrać aplikację. Urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Wersja aplikacji**

  Pole, w którym możesz określić wersję wybranej aplikacji.

- **Producent**

  Lista rozwijalna, z której możesz wybrać producenta aplikacji zainstalowanej na urządzeniu.

- **Stan aplikacji**

  Lista rozwijalna, z której możesz wybrać stan aplikacji (*Zainstalowana*, *Nie zainstalowana*). Urządzenia, na których określona aplikacja została zainstalowana lub nie została zainstalowana, w zależności od wybranego stanu, zostaną uwzględnione w wyborze.

- **Wyszukaj według aktualizacji**

  Jeśli ta opcja jest włączona, wyszukiwanie będzie się odbywać z użyciem szczegółów aktualizacji dla aplikacji zainstalowanych na odpowiednich urządzeniach. Po zaznaczeniu pola, pola **Nazwa aplikacji**, **Wersja aplikacji** i **Stan aplikacji** zostaną zmienione na **Nazwa aktualizacji**, **Wersja aktualizacji** i **Stan**.

  Domyślnie opcja ta jest wyłączona.

- **Nazwa niekompatybilnej aplikacji zabezpieczającej**

  Lista rozwijalna, z której możesz wybrać aplikacje zabezpieczające firm trzecich. Podczas wyszukiwania, urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Znacznik aplikacji**

  Z listy rozwijalnej możesz wybrać znacznik aplikacji. Wszystkie urządzenia, na których są zainstalowane aplikacje z wybranym znacznikiem w opisie, zostają uwzględnione w wyborze urządzeń.

Hierarchia Serwerów administracyjnych

Na zakładce **Hierarchia Serwerów administracyjnych** zaznacz pole **Uwzględnij dane z podrzędnych Serwerów administracyjnych (do poziomu)**, jeśli chcesz, żeby informacje przechowywane na podrzędnych Serwerach administracyjnych były brane pod uwagę podczas wyszukiwania urządzeń, a w polu wejściowym możesz określić poziom zagnieżdżenia podrzędnego Serwera administracyjnego, z którego informacje są brane pod uwagę podczas wyszukiwania urządzeń. Domyślnie pole to nie jest zaznaczone.

Maszyny wirtualne

Na zakładce **Maszyny wirtualne** możesz skonfigurować wyszukiwanie urządzeń w zależności od tego, czy są to maszyny wirtualne lub czy są one częścią infrastruktury pulpitu wirtualnego (VDI):

- **Jest maszyną wirtualną**

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Wyszukuje urządzenia, które są maszynami wirtualnymi.

- Typ maszyny wirtualnej

  Z listy rozwijalnej możesz wybrać producenta maszyny wirtualnej.

  Ta lista rozwijalna jest dostępna, jeśli wartość **Tak** lub **Nieważne** została wybrana na liście rozwijalnej **Jest maszyną wirtualną**.

- Część Virtual Desktop Infrastructure

  Z listy rozwijalnej możesz wybrać następujące opcje:

  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są częścią Virtual Desktop Infrastructure.
  - **Tak**. Wyszukuje urządzenia, które są częścią Virtual Desktop Infrastructure (VDI).

Sprzęt

Na zakładce **Sprzęt** możesz skonfigurować wyszukiwanie urządzeń klienckich według ich sprzętu:

- Urządzenie

  Z listy rozwijalnej możesz wybrać typ jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- Producent

  Z listy rozwijalnej możesz wybrać nazwę producenta jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- Opis

  Opis urządzenia lub sprzętu. Urządzenia z opisem określonym w tym polu zostaną uwzględnione w wyborze.

  Opis urządzenia w dowolnym formacie może zostać wprowadzony w oknie właściwości tego urządzenia. Pole obsługuje wyszukiwanie pełnotekstowe.

- Numer ewidencyjny

  Sprzęt o numerze inwentarzowym podanym w tym polu zostanie uwzględniony w wyborze.

- Częstotliwość procesora, w MHz

  Zakres częstotliwości procesora. Urządzenia z procesorami odpowiadającymi zakresowi częstotliwości określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- Wirtualne rdzenie procesora

  Zakres liczby wirtualnych rdzeni w procesorze. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- Pojemność dysku twardego, w GB

  Zakres wartości rozmiaru dysku twardego urządzenia. Urządzenia z dyskami twardymi odpowiadającymi zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

- Rozmiar pamięci RAM, w MB

  Zakres wartości rozmiaru pamięci RAM urządzenia. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

Luki oraz aktualizacje

Na zakładce **Luki oraz aktualizacje** możesz skonfigurować kryteria wyszukiwania urządzeń zgodnie z ich źródłem Windows Update:

- WUA został przełączony na Serwer administracyjny

  Z listy rozwijalnej można wybrać jedną z następujących opcji wyszukiwania:
  - **Tak**. Jeśli wybrano tę opcję, wyniki wyszukiwania będą uwzględniać urządzenia, które uzyskały aktualizacje poprzez Windows Update z Serwera administracyjnego.
  - **Nie**. Jeśli wybrano tę opcję, wyniki będą uwzględniać urządzenia, które uzyskały aktualizacje za pośrednictwem Windows Update z innych źródeł.

Użytkownicy

Na zakładce **Użytkownicy** możesz skonfigurować kryteria wyszukiwania urządzeń według kont użytkowników, którzy logowali się do systemu operacyjnego.

- Ostatni użytkownik zalogowany do systemu

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik ostatnio logował się do systemu.

- Użytkownik zalogowany do systemu co najmniej raz

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik przynajmniej raz logował się do systemu.

Problemy mające wpływ na stan zarządzanych aplikacji

Na zakładce **Problemy mające wpływ na stan zarządzanych aplikacji** możesz skonfigurować wyszukiwanie urządzeń według opisów ich stanów dostarczonych przez zarządzane aplikacje:

- **Opis stanu urządzenia**

  Możesz zaznaczyć opcje dla opisów stanów z zarządzanej aplikacji. Po odebraniu tych stanów, urządzenia zostaną uwzględnione w wyborze. Jeśli wybierzesz stan wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego stanu na wszystkich listach.

Stan komponentów w zarządzanych aplikacjach

Na zakładce **Stan komponentów w zarządzanych aplikacjach** możesz skonfigurować kryteria wyszukiwania urządzeń według stanów komponentów w zarządzanych aplikacjach:

- **Stan ochrony przed wyciekiem danych**

  Wyszukiwanie urządzeń według stanu Ochrona przed wyciekaniem danych (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymano, Uruchomione, Niepowodzenie*).

- **Stan ochrony serwerów współpracy**

  Wyszukiwanie urządzeń według stanu ochrony serwerów współpracy (*Brak danych z urządzenia*, *Zatrzymana*, *Uruchamianie, Wstrzymano*, *Uruchomione*, *Niepowodzenie*).

- **Stan ochrony antywirusowej serwerów pocztowych**

  Wyszukiwanie urządzeń według stanu ochrony dla serwerów pocztowych (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymano, Uruchomione, Niepowodzenie*).

- **Stan czujnika Endpoint Sensor**

  Wyszukiwanie urządzeń według stanu komponentu Endpoint Sensor (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymano, Uruchomione, Niepowodzenie*).

Szyfrowanie

- **Szyfrowanie**

  Algorytm blokowego szyfru symetrycznego AES (Advanced Encryption Standard). Z listy rozwijalnej możesz wybrać długość klucza szyfrowania (56-bitowy, 128-bitowy, 192-bitowy lub 256-bitowy).

  Dostępne wartości: *AES56*, *AES128*, *AES192* i *AES256*.

Segmenty chmury

Na zakładce **Segmenty chmury** możesz skonfigurować wyszukiwanie w oparciu o przynależność urządzenia do określonych segmentów chmury:

- **Urządzenie znajduje się w segmencie chmury**

Jeśli ta opcja jest włączona, możesz kliknąć przycisk **Przeglądaj**, aby określić przeszukiwany segment.

Jeśli włączono także opcję **Włączając obiekty potomne**, wyszukiwanie jest uruchamiane na wszystkich obiektach potomnych określonego segmentu.

Wyniki wyszukiwania zawierają tylko urządzenia z wybranego segmentu.

- Urządzenie wykryte przy pomocy API

  Z listy rozwijalnej możesz wybrać, czy urządzenie jest wykrywane przez narzędzia API:

  - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.
  - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.
  - **Google Cloud.** Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku Google Cloud.
  - **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale nie może zostać wykryte przy użyciu API.
  - **Brak wartości**. Warunek nie ma zastosowania.

Składniki aplikacji

Ta sekcja zawiera listę komponentów tych aplikacji, które posiadają odpowiednie wtyczki administracyjne, zainstalowane w Konsoli administracyjnej.

W sekcji **Składniki aplikacji** możesz określić kryteria uwzględniania urządzeń w wyborze zgodnie ze stanami i numerami wersji komponentów, które odpowiadają wybranej aplikacji:

- Stan

Wyszukiwanie urządzeń zgodnie ze stanem komponentu wysłanym przez aplikację do Serwera administracyjnego. Możesz wybrać jeden z następujących stanów: *Brak danych z urządzenia*, *Zatrzymane*, *Uruchamianie*, *Wstrzymane*, *Uruchomione*, *Błąd* lub *Nie zainstalowano*. Jeśli wybrany komponent aplikacji zainstalowanej na zarządzanym urządzeniu posiada określony stan, urządzenie jest uwzględniane w wyborze urządzeń.

Stany wysłane przez aplikacje:

- *Uruchamianie*—komponent jest właśnie w procesie inicjalizacji.
- *Uruchomione*—komponent jest włączony i działa poprawnie.
- *Wstrzymane*—komponent został zawieszony, na przykład, po wstrzymaniu przez użytkownika ochrony w zarządzanej aplikacji.
- *Błąd*—podczas działania komponentu wystąpił błąd.
- *Zatrzymane*—komponent jest wyłączony i nie działa w tym momencie.
- *Nie zainstalowano*—użytkownik nie wybrał komponentu do zainstalowania podczas konfigurowania niestandardowej instalacji aplikacji.

W przeciwieństwie do pozostałych stanów, stan *Brak danych z urządzenia* nie jest wysyłany przez aplikacje. Ta opcja pokazuje, że aplikacje nie posiadają informacji o wybranym stanie komponentu. Na przykład, to może mieć miejsce, gdy wybrany komponent nie należy do żadnej z aplikacji zainstalowanych na urządzeniu lub gdy urządzenie jest wyłączone.

- **Wersja**

  Wyszukiwanie urządzeń zgodnie z numerem wersji komponentu, który wybierasz na liście. Możesz wpisać numer wersji, na przykład `3.4.1.0`, a następnie określić, czy wybrany komponent musi posiadać równą, wcześniejszą lub nowszą wersję. Możesz także skonfigurować wyszukiwanie wszystkich wersji, za wyjątkiem określonej.

Używanie masek w zmiennych typu string

Używanie masek w zmiennych typu string jest dozwolone. Podczas tworzenia masek można użyć następujących wyrażeń regularnych:

- Symbol wieloznaczny (*)—oznacza dowolną sekwencję 0 lub kilku znaków.
- Znak zapytania (?)—zastępuje dowolny pojedynczy znak.
- [<range>]—zastępuje dowolny pojedynczy znak z podanego zakresu lub zbioru.

  Na przykład: [0–9] — dowolna cyfra. [abcdef] — dowolny ze znaków a, b, c, d, e lub f.

Używanie wyrażeń regularnych w polu wyszukiwania

W celu wyszukania określonych słów i znaków, w polu wyszukiwania użyj następujących wyrażeń regularnych:

- *. Zastępuje dowolną sekwencję znaków. Aby wyszukać słowa Serwer, Serwery lub Serwerownia, w polu wyszukiwania wpisz `Server*`.
- ?. Zastępuje dowolny pojedynczy znak. Aby wyszukać słowa Word lub Ward, w polu wyszukiwania wpisz `W?rd`.

  > Tekst znajdujący się w polu wyszukiwania nie może rozpoczynać się od znaku zapytania (?).

- [<zakres>]. Zastępuje dowolny pojedynczy znak z podanego zakresu lub zbioru. Aby wyszukać dowolną cyfrę, w polu wyszukiwania wpisz `[0-9]`. Aby wyszukać jeden ze znaków—a, b, c, d, e lub f— w polu wyszukiwania wpisz `[abcdef]`.

W celu uruchomienia wyszukiwania pełnotekstowego, w polu wyszukiwania użyj następujących wyrażeń regularnych:

- Spacji. Wynikiem są wszystkie urządzenia, których opisy zawierają dowolne z wymienionych słów. Na przykład, aby wyszukać frazę, która zawiera słowo „Podrzędny" lub „Wirtualny": (lub oba te słowa), w polu wyszukiwania wpisz wyrażenie `Secondary Virtual`.
- Znak plusa (+), I lub &&. Jeśli przed wyrazem wpisano znak "+", wszystkie wyniki wyszukiwania będą zawierać ten wyraz. Na przykład, aby wyszukać frazę, która zawiera słowa „Podrzędny" i „Wirtualny", w polu wyszukiwania możesz wpisać jedno z następujących wyrażeń: `+Secondary+Virtual`, `Secondary AND Virtual`, `Secondary && Virtual`.
- LUB lub ||. Jeśli te symbole znajdują się między dwoma słowami, oznacza to, że jedno lub drugie słowo można znaleźć w tekście. Aby wyszukać frazę, która zawiera słowo „Podrzędny" lub „Wirtualny", w polu wyszukiwania wpisz jedno z następujących wyrażeń: `Secondary OR Virtual`, `Secondary || Virtual`.
- Znak minusa (-). Jeśli przed wyrazem wpisano znak "-", żaden z wyników wyszukiwania nie będzie zawierać tego wyrazu. Aby wyszukać frazę, która musi zawierać słowo Podrzędny, a nie może zawierać słowa Wirtualny, w polu wyszukiwania wpisz `+Secondary-Virtual`.
- `"<jakikolwiek tekst>"`. Tekst w cudzysłowach musi znajdować się w tekście. Aby wyszukać frazę, która zawiera kombinację słów Podrzędny Serwer, w polu wyszukiwania wpisz `"Secondary Server"`.

Wyszukiwanie pełnotekstowe jest dostępne w następujących sekcjach filtrowania:

- W sekcji filtrowania listy zdarzeń, według kolumn **Zdarzenie** i **Opis**.
- W sekcji filtrowania konta użytkownika, według kolumny **Nazwa**.
- W sekcji filtrowania rejestru aplikacji, według kolumny **Nazwa**, jeśli w sekcji **Pokaż na liście** jako warunek filtrowania wybrano **brak grupowania**.

Eksportowanie list z okien dialogowych

W oknach dialogowych aplikacji możesz wyeksportować listy obiektów do plików tekstowych.

Eksportowanie listy obiektów jest możliwe w sekcjach okien dialogowych, które zawierają przycisk **Eksportuj do pliku**.

Ustawienia zadań

Ta sekcja wyświetla wszystkie ustawienia zadań w Kaspersky Security Center.

Ogólne ustawienia zadania

Ta sekcja zawiera ustawienia, które możesz przeglądać i konfigurować dla większości swoich zadań. Lista dostępnych ustawień zależy od konfigurowanego zadania.

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- Ustawienia ponownego uruchamiania systemu operacyjnego:
  - **Nie uruchamiaj ponownie urządzenia**

    Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

  - **Uruchom urządzenie ponownie**

    Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

  - **Pytaj użytkownika o akcję**

    Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

    Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Uruchom ponownie po (min)**

Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- Wymuś zamknięcie aplikacji dla zablokowanych sesji

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

- Ustawienia terminarza zadania:

  - **Ustawienia Zaplanowane uruchomienie**

    - Co N godzin

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

      Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

    - Co N dni

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

      Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

    - Co N tygodni

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

      Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

    - Co N minut

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

      Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po pobraniu nowych uaktualnień do repozytorium**

  Zadanie jest uruchamiane po pobraniu uaktualnień do repozytorium. Na przykład, możesz użyć tego terminarza dla zadania wyszukiwania luk i wymaganych aktualizacji.

- **Po epidemii wirusa**

Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

- Ochrona antywirusowa stacji roboczych i serwerów plików
- Ochrona antywirusowa bram internetowych
- Ochrona antywirusowa serwerów pocztowych

Domyślnie, zaznaczone są wszystkie typy aplikacji.

Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest włączona.

- Używaj automatycznie losowego opóźnienia dla uruchamiania zadań

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

- Urządzenia, do których zadanie zostanie przypisane:
  - **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**

    Zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

    Na przykład, możesz chcieć użyć tej opcji w zadaniu instalowania Agenta sieciowego na nieprzypisanych urządzeniach.

  - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

    Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

    Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

  - **Przypisz zadanie do wyboru urządzeń**

    Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

    Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

  - **Przypisz zadanie do grupy administracyjnej**

    Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

    Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

- Ustawienia konta:
  - **Konto domyślne**

    Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

    Domyślnie opcja ta jest zaznaczona.

  - **Określ konto**

Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

- **Konto**

  Konto, z poziomu którego zadanie jest uruchamiane.

- **Hasło**

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

Ustawienia określone po utworzeniu zadania

Następujące ustawienia możesz określić tylko po utworzeniu zadania.

- Ustawienia zadań grupowych:

  - **Roześlij do podgrup**

    Ta opcja jest dostępna tylko w ustawieniach zadań grupowych.

    Kiedy ta opcja jest włączona, zakres zadania obejmuje:

    - Grupa administracyjna, którą wybrano podczas tworzenia zadania.
    - Grupy administracyjne podporządkowane wybranej grupie administracyjnej na dowolnym poziomie niżej w hierarchii grup.

    Gdy ta opcja jest wyłączona, zakres zadania obejmuje tylko grupę administracyjną wybraną podczas tworzenia zadania.

    Domyślnie opcja ta jest włączona.

  - **Wyślij do podrzędnych i wirtualnych Serwerów administracyjnych**

    Gdy ta opcja jest włączona, zadanie działające na podstawowym serwerze administracyjnym jest również stosowane na pomocniczych (drugorzędnych) serwerach administracyjnych (w tym wirtualnych). Jeżeli zadanie tego samego typu już istnieje na pomocniczym serwerze administracyjnym, oba zadania są stosowane na pomocniczym serwerze administracyjnym — istniejące i odziedziczone z podstawowego serwera administracyjnego.

    Ta opcja jest dostępna tylko wtedy, gdy włączona jest opcja **Roześlij do podgrup**.

    Domyślnie opcja ta jest wyłączona.

- Zaawansowane ustawienia terminarza:

  - **Włącz urządzenia przed uruchomieniem zadania (min) przy użyciu funkcji Wake-on-LAN**

System operacyjny na urządzeniu zostanie uruchomiony o określonym czasie przed uruchomieniem zadania. Domyślnie czas ten wynosi pięć minut.

Włącz tę opcję, jeśli chcesz, aby zadanie było uruchamiane na wszystkich urządzeniach klienckich z obszaru zadania, w tym tych urządzeniach, które są wyłączone, gdy zadanie ma zostać uruchomione.

Jeśli chcesz, żeby urządzenie było automatycznie wyłączane po zakończeniu zadania, włącz opcję **Wyłącz urządzenia po zakończeniu zadania**. Ta opcja znajduje się w tym samym oknie.

Domyślnie opcja ta jest wyłączona.

- Wyłącz urządzenia po zakończeniu zadania

  Na przykład, możesz chcieć włączyć tę opcję dla zadania instalacji aktualizacji, które instaluje uaktualnienia na urządzeniach klienckich w każdy piątek w godzinach pracy, a następnie wyłącza te urządzenia w weekend.

  Domyślnie opcja ta jest wyłączona.

- Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż (min)

  Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

  Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

  Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.

- Ustawienia powiadomień:
  - Sekcja **Przechowywanie historii zadania**:
    - Na Serwerze administracyjnym przez (dni)

      Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane na Serwerze administracyjnym przez określoną liczbę dni. Po upłynięciu tego okresu, informacje są usuwane z Serwera administracyjnego.

      Domyślnie opcja ta jest włączona.

    - Przechowuj w systemowym dzienniku zdarzeń urządzenia

      Zdarzenia aplikacji związane z wykonaniem zadania są przechowywane lokalnie w dzienniku zdarzeń systemu Windows każdego urządzenia klienckiego.

      Domyślnie opcja ta jest wyłączona.

    - Przechowuj w systemowym dzienniku zdarzeń Serwera administracyjnego

Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane w sposób scentralizowany w dzienniku zdarzeń Windows systemu operacyjnego Serwera administracyjnego.

Domyślnie opcja ta jest wyłączona.

- **Zapisz wszystkie zdarzenia**

  Jeśli ta opcja jest zaznaczona, wszystkie zdarzenia dotyczące zadania zostaną zapisane w dziennikach zdarzeń.

- **Zapisz zdarzenia dotyczące postępu zadania**

  Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wykonania zadania zostaną zapisane w dziennikach zdarzeń.

- **Zapisz jedynie wyniki wykonywania zadania**

  Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wyników zadania zostaną zapisane w dziennikach zdarzeń.

- **Powiadom administratora o wynikach wykonywania zadania**

  Możesz wybrać metody, przy użyciu których administratorzy otrzymają powiadomienia o wynikach wykonania zadań: za pośrednictwem poczty elektronicznej, przez SMS oraz poprzez uruchomienie pliku wykonywalnego. Aby skonfigurować powiadomienie, kliknij odnośnik **Ustawienia**.

  Domyślnie, wszystkie metody powiadamiania są wyłączone.

- **Powiadom tylko o błędach**

  Jeśli ta opcja jest włączona, administratorzy są powiadamiani tylko wtedy, gdy wykonanie zadania zakończy się błędem.

  Jeśli ta opcja jest wyłączona, administratorzy są powiadamiania po każdym zakończeniu wykonywania zadania.

  Domyślnie opcja ta jest włączona.

- Ustawienia zabezpieczeń
- Ustawienia obszaru zadania

  W zależności od sposobu określenia obszaru zadania, dostępne są następujące ustawienia:

  - **Urządzenia**

    Jeśli obszar zadania jest określany przez grupę administracyjną, możesz przejrzeć tę grupę. Nie ma tutaj dostępnych zmian. Jednakże możesz ustawić **Wykluczenia z zakresu zadania**.

    Jeśli obszar zadania jest określany przez listę urządzeń, możesz zmodyfikować tę listę poprzez dodanie i usunięcie urządzeń.

- Wybór urządzeń

  Możesz zmienić wybór urządzeń, do którego zadanie jest stosowane.

- Wykluczenia z zakresu zadania

  Możesz określić grupę urządzeń, do których zadanie nie jest stosowane. Grupy, które mają zostać wykluczone, mogą być tylko podgrupami grupami administracyjnej, do której zadanie jest stosowane.

- **Historia rewizji**

Ustawienia zadania pobierania aktualizacji do repozytorium serwera administracyjnego

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- Źródła aktualizacji

  Jako źródła uaktualnień dla Serwera administracyjnego można użyć następujących zasobów:

  - Serwery aktualizacji Kaspersky

    Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji. Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

    Ta opcja jest wybrana domyślnie.

  - Główny Serwer administracyjny

    Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

  - Folder lokalny lub sieciowy

    Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

    Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

- **Inne ustawienia**

  Wymuś aktualizację podrzędnych Serwerów administracyjnych

Jeżeli ta opcja jest włączona, Serwer administracyjny uruchomi zadania aktualizacji na podrzędnych Serwerach administracyjnych zaraz po pobraniu nowych aktualizacji. W innym przypadku zadania aktualizacji na podrzędnych Serwerach administracyjnych będą uruchamiane zgodnie ze swoimi terminarzami.

Domyślnie opcja ta jest wyłączona.

Kopiuj pobrane aktualizacje do dodatkowych folderów

Po otrzymaniu przez Serwer administracyjny uaktualnień skopiuje on je do określonych folderów. Użyj tej opcji, jeśli chcesz ręcznie zarządzać dystrybucją uaktualnień w sieci.

Na przykład, chcesz użyć tej opcji w następującej sytuacji: sieć Twojej organizacji zawiera kilka niezależnych podsieci, a urządzenia z każdej podsieci nie mają dostępu do innych podsieci. Jednakże urządzenia we wszystkich podsieciach mają dostęp do wspólnego udziału sieciowego. W tym przypadku skonfiguruj Serwer administracyjny w jednej z podsieci tak, aby pobierał uaktualnienia z serwerów aktualizacji Kaspersky, włącz tę opcję, a następnie określ ten udział sieciowy. W zadaniach pobierania uaktualnień do repozytorium dla innych Serwerów administracyjnych określ ten sam udział sieciowy jako źródło uaktualnień.

Domyślnie opcja ta jest wyłączona.

Nie wymuszaj aktualizacji urządzeń i podrzędnych Serwerów administracyjnych przed zakończeniem kopiowania

Zadania pobierania aktualizacji na urządzenia klienckie i podrzędne Serwery administracyjne zostaną uruchomione dopiero po skopiowaniu aktualizacji z głównego folderu aktualizacji do dodatkowych folderów aktualizacji.

Ta opcja musi być włączona, jeśli urządzenia klienckie i podrzędne Serwery administracyjne pobierają aktualizacje z dodatkowych folderów sieciowych.

Domyślnie opcja ta jest wyłączona.

Ustawienia określone po utworzeniu zadania

Następujące ustawienia możesz określić tylko po utworzeniu zadania.

- Sekcja **Ustawienia**, sekcja **Zawartość aktualizacji**

  Pobierz pliki diff

  Ta opcja włącza funkcję pobierania plików diff.

  Domyślnie opcja ta jest wyłączona.

- Sekcja **Weryfikacja uaktualnień**

  Zweryfikuj uaktualnienia przed rozesłaniem

Serwer administracyjny pobiera uaktualnienia ze źródła, zapisuje je w tymczasowym repozytorium i uruchamia zadanie określone w polu **Zadanie weryfikacji uaktualnień**. Jeśli zadanie zakończy się pomyślnie, uaktualnienia są kopiowane z tymczasowego repozytorium do folderu współdzielonego na Serwerze administracyjnym, a następnie są rozsyłane do wszystkich urządzeń, dla których Serwer administracyjny pełni rolę źródła uaktualnień (zadania są uruchamiane zgodnie z opcją terminarza - **Po pobraniu nowych uaktualnień do repozytorium**). Zadanie pobierania uaktualnień do repozytorium zostaje zakończone dopiero po zakończeniu zadania *weryfikacji uaktualnień*.

Domyślnie opcja ta jest wyłączona.

Zadanie weryfikacji uaktualnień

To zadanie weryfikuje pobrane uaktualnienia przed ich rozesłaniem na wszystkie urządzenia, dla których Serwer administracyjny pełni rolę źródła uaktualnień.

W tym polu możesz określić utworzone wcześniej zadanie *weryfikacji uaktualnień*. Ewentualnie możesz utworzyć nowe zadanie *weryfikacji uaktualnień*.

Ustawienia zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- **Źródła aktualizacji**

  Jako źródła uaktualnień dla punktu dystrybucji można użyć następujących zasobów:

  - Serwery aktualizacji Kaspersky

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

    Opcja ta jest wybrana domyślnie.

  - Główny Serwer administracyjny

    Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

  - Folder lokalny lub sieciowy

    Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

    Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

- **Inne ustawienia** → Folder do przechowywania aktualizacji

  Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

Ustawienia określone po utworzeniu zadania

Poniższe ustawienie możesz określić w sekcji **Ustawienia**, w bloku **Zawartość aktualizacji** dopiero po utworzeniu zadania.

Pobierz pliki diff

Ta opcja włącza funkcję pobierania plików diff.

Domyślnie opcja ta jest wyłączona.

Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft

  Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

  Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

  - Połącz z serwerem aktualizacji, aby zaktualizować dane

Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł uaktualnień Microsoft:

- Serwer administracyjny Kaspersky Security Center (zapoznaj się z ustawieniami profilu Agenta sieciowego)
- System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
- Serwery aktualizacji Microsoft

Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła uaktualnień Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach profilu Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

Domyślnie opcja ta jest włączona.

Kombinacja następujących opcji ustawień profilu Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

- Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie z serwerem aktualizacji, aby uzyskać aktualizacje tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona, a opcja **Aktywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została zaznaczona.
- Agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła uaktualnień Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia, jeśli opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** została włączona, a opcja **Pasywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została wybrana, jeśli opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest wyłączona, a opcja **Aktywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została zaznaczona.
- Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Wyłączono** w ustawieniach grupy **Tryb wyszukiwania aktualizacji systemu Windows** jest zaznaczona, Kaspersky Security Center nie żąda żadnych informacji o aktualizacjach.

- Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky

Jeśli ta opcja jest włączona, Kaspersky Security Center wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

Domyślnie opcja ta jest włączona.

- Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików

  Foldery, w których Kaspersky Security Center wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

  Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

- Włącz diagnostykę zaawansowaną

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

Ustawienia zadania Zainstaluj wymagane aktualizacje i napraw luki

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- Określ reguły instalacji aktualizacji

  Te reguły są stosowane do instalacji aktualizacji na urządzeniach klienckich. Jeśli reguły nie zostały określone, zadanie nie zostanie wykonane. Informacje dotyczące działań wykonywanych na regułach znajdziesz w sekcji Reguły instalacji aktualizacji.

- Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia

  Jeśli ta opcja jest włączona, aktualizacje są instalowane po ponownym uruchomieniu lub zamknięciu urządzenia. W innym przypadku aktualizacje są instalowane zgodnie z terminarzem.

  Użyj tej opcji, jeśli instalowanie aktualizacji może wpłynąć na działanie urządzenia.

  Domyślnie opcja ta jest wyłączona.

- **Zainstaluj wymagane ogólne składniki systemu**

  Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

  Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

  Domyślnie opcja ta jest wyłączona.

- **Zezwól na instalację nowych wersji aplikacji podczas aktualizacji**

  Jeśli ta opcja jest włączona, aktualizacje są dozwolone, gdy powodują zainstalowanie nowej wersji aplikacji.

  Jeśli ta opcja jest wyłączona, aplikacja nie zostanie zaktualizowana. W takiej sytuacji możesz ręcznie zainstalować nowe wersje aplikacji lub użyć w tym celu innego zadania. Na przykład, możesz użyć tej opcji, jeśli struktura Twojej firmy nie jest obsługiwana przez nową wersję aplikacji lub jeśli chcesz sprawdzić aktualizację w infrastrukturze testowej.

  Domyślnie opcja ta jest włączona.

  > Aktualizowanie aplikacji może spowodować problemy z działaniem powiązanych aplikacji zainstalowanych na urządzeniach klienckich.

- **Pobierz aktualizacje na urządzenie, ale ich nie instaluj**

  Jeśli ta opcja jest włączona, aplikacja pobierze uaktualnienia na urządzenie, ale nie zainstaluje ich automatycznie. Możesz ręcznie zainstalować pobrane aktualizacje.

  Aktualizacje Microsoft są pobierane do folderu systemowego Windows. Aktualizacje aplikacji firm trzecich (aplikacje innych producentów niż Kaspersky i Microsoft) są pobierane do folderu określonego w polu **Folder do pobierania aktualizacji**.

  Jeśli ta opcja jest wyłączona, aktualizacje są instalowane na urządzeniu automatycznie.

  Domyślnie opcja ta jest wyłączona.

  - **Folder do pobierania aktualizacji**

    > Ten folder jest używany do pobierania aktualizacji aplikacji innych firm (aplikacji innych producentów niż Kaspersky i Microsoft).

- **Włącz diagnostykę zaawansowaną**

Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

Ustawienia określone po utworzeniu zadania

Ustawienia w sekcjach wymienionych poniżej można określić dopiero po utworzeniu zadania. Aby uzyskać pełny opis ustawień zadania, zobacz Ogólne ustawienia zadania.

- **Ogólny**. W tej sekcji wyświetlane są ogólne informacje o zadaniu. Możesz także określić, do których urządzeń powinno zostać zastosowane zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

  - **Roześlij do podgrup**

    Ta opcja jest dostępna tylko w ustawieniach zadań grupowych.

    Kiedy ta opcja jest włączona, zakres zadania obejmuje:

    - Grupa administracyjna, którą wybrano podczas tworzenia zadania.
    - Grupy administracyjne podporządkowane wybranej grupie administracyjnej na dowolnym poziomie niżej w hierarchii grup.

    Gdy ta opcja jest wyłączona, zakres zadania obejmuje tylko grupę administracyjną wybraną podczas tworzenia zadania.

    Domyślnie opcja ta jest włączona.

  - **Wyślij do podrzędnych i wirtualnych Serwerów administracyjnych**

    Gdy ta opcja jest włączona, zadanie działające na podstawowym serwerze administracyjnym jest również stosowane na pomocniczych (drugorzędnych) serwerach administracyjnych (w tym wirtualnych). Jeżeli zadanie tego samego typu już istnieje na pomocniczym serwerze administracyjnym, oba zadania są stosowane na pomocniczym serwerze administracyjnym — istniejące i odziedziczone z podstawowego serwera administracyjnego.

    Ta opcja jest dostępna tylko wtedy, gdy włączona jest opcja **Roześlij do podgrup**.

    Domyślnie opcja ta jest wyłączona.

- Aktualizacje do zainstalowania

  W sekcji **Aktualizacje do zainstalowania** możesz przejrzeć listę aktualizacji instalowanych przez zadanie. Wyświetlane są tylko aktualizacje, które odpowiadają zastosowanych ustawieniom zadania.

- Testowa instalacja aktualizacji:

  - **Nie skanuj**. Wybierz tę opcję, jeśli nie chcesz przeprowadzać testowej instalacji aktualizacji.

  - **Uruchom skanowanie na wybranych urządzeniach**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na wybranych urządzeniach. Kliknij przycisk **Dodaj** i wybierz urządzenia, na których chcesz przeprowadzić testową instalację aktualizacji.

  - **Uruchom skanowanie na urządzeniach w określonej grupie**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na grupach urządzeń. W polu **Określ grupę testową** określ grupę urządzeń, na których chcesz przeprowadzić instalację testową.

  - **Uruchom skanowanie na określonym procencie urządzeń**. Wybierz tę opcję, jeśli chcesz przetestować instalację aktualizacji na określonej liczbie urządzeń. W polu **Procentowy udział urządzeń testowych z wszystkich urządzeń docelowych** określ procentową ilość urządzeń, na których chcesz przeprowadzić testową instalację aktualizacji.

Globalna lista podsieci

Ta sekcja zawiera informacje o globalnej liście podsieci, których możesz użyć w regułach.

Aby przechowywać informacje o podsieciach w Twojej sieci, możesz skonfigurować globalną listę podsieci dla każdego używanego Serwera administracyjnego. Ta lista pomaga w dopasowaniu par {adres IP, maska} i fizycznych jednostek, takich jak oddziały firmy. Możesz użyć podsieci z tej listy w ustawieniach i regułach sieci.

Dodawanie podsieci do globalnej listy podsieci

Możesz dodać podsieci z ich opisami do globalnej listy podsieci.

W celu dodania podsieci do globalnej listy podsieci:

1. W drzewie konsoli wybierz węzeł Serwera administracyjnego, którego potrzebujesz.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W otwartym oknie **właściwości**, w panelu **Sekcje** wybierz **Lista globalnych podsieci**.
4. Kliknij przycisk **Dodaj**.

   Zostanie otwarte okno **Nowa podsieć**.
5. Wypełnij następujące pola:

   - Ustawienia ogólne

     Adres IP dodawanej podsieci.

- **Maska podsieci**

  Maska dodawanej podsieci.

- **Nazwa**

  Nazwa podsieci. Musi być unikatowa w obrębie globalnej listy podsieci. Jeśli wprowadzisz nazwę, która już istnieje na liście, zostanie dodany indeks, na przykład: ~~1, ~~2.

- **Opis**

  Opis może zawierać dodatkowe informacje o oddziale firmy, który posiada tę podsieć. Ten tekst pojawi się na wszystkich listach, gdzie ta podsieć jest obecna, na przykład, na liście reguł ograniczających ruch sieciowy.

  To pole nie jest obowiązkowe i może pozostać puste.

6. Kliknij **OK**.

Podsieć pojawi się na liście podsieci.

Przeglądanie i modyfikowanie właściwości podsieci z globalnej listy podsieci

Możesz przejrzeć i zmodyfikować właściwości podsieci na globalnej liście podsieci.

W celu przejrzenia lub zmodyfikowania właściwości podsieci na globalnej liście podsieci:

1. W drzewie konsoli wybierz węzeł Serwera administracyjnego, którego potrzebujesz.
2. Z menu kontekstowego Serwera administracyjnego wybierz **Właściwości**.
3. W otwartym oknie **Właściwości**, w lewym panelu **Sekcje** wybierz **Lista globalnych podsieci**.
4. Z listy wybierz żądaną podsieć.
5. Kliknij przycisk **Właściwości**.
   Zostanie otwarte okno **Nowa podsieć**.
6. Jeśli to konieczne, zmień ustawienia podsieci.
7. Kliknij **OK**.

Jeśli wprowadziłeś zmiany, zostaną zachowane.

Korzystanie z Agenta sieciowego dla systemu Windows, macOS i Linux: porównanie

Korzystanie z Agenta sieciowego różni się w zależności od systemu operacyjnego urządzenia. Ustawienia zasady Agenta sieciowego i pakietu instalacyjnego także różnią się w zależności od systemu operacyjnego. W poniższej tabeli porównano funkcje Agenta sieciowego i scenariusze użycia dostępne dla systemów operacyjnych Windows, macOS i Linux.

Porównanie funkcji Agenta sieciowego

Funkcja Agenta sieciowego	Windows	macOS	Linux
Instalacja			
Automatyczne tworzenie pakietu instalacyjnego Agenta sieciowego po zainstalowaniu Kaspersky Security Center	✓	–	–
Instalowanie w trybie wymuszonym, korzystając ze specjalnych opcji w zadaniu zdalnej instalacji programu Kaspersky Security Center	✓	✓	✓
Instalowanie poprzez wysyłanie do użytkowników urządzeń odnośników do pakietów autonomicznych, wygenerowanych przez Kaspersky Security Center	✓	✓	✓
Instalowanie poprzez klonowanie obrazu dysku twardego administratora z systemem operacyjnym i Agentem sieciowym przy pomocy narzędzi do zarządzania obrazami dysku, dostępnych w Kaspersky Security Center	✓	–	–
Instalacja poprzez sklonowanie obrazu dysku twardego administratora z systemem operacyjnym i Agentem sieciowym przy użyciu narzędzi innych firm	✓	✓	✓
Instalowanie przy użyciu narzędzi firm trzecich dla zdalnej instalacji aplikacji	✓	✓	✓
Ręczne instalowanie poprzez uruchomienie instalatorów aplikacji na urządzeniach	✓	✓	✓
Instalowanie Agenta sieciowego w trybie cichym	✓	✓	✓
Instalowanie Agenta sieciowego w trybie nieinteraktywnym	✓	✓	✓

Ręczne łączenie urządzenia klienckiego z Serwerem administracyjnym. Narzędzie klmover	✓	✓	✓
Automatyczne instalowanie aktualizacji i poprawek dla komponentów Kaspersky Security Center	✓	–	–
Automatyczne rozsyłanie kluczy	✓	✓	✓
Wymuszona synchronizacja	✓	✓	✓
Punkt dystrybucji			
Przy użyciu punktu dystrybucji	✓	✓	✓
Automatyczne przypisywanie punktów dystrybucji	✓	✓ Bez korzystania z uwierzytelniania na poziomie sieci (NLA).	✓ Bez korzystania z uwierzytelniania na poziomie sieci (NLA).
Tryb offline pobierania uaktualnień	✓	✓	✓
Przeszukiwanie sieci	✓ • Przeszukiwanie zakresu IP • Przeszukiwanie sieci Windows • Przeszukiwanie Active Directory	–	✓ Przeszukiwanie zakresu IP
Uruchamianie usługi KSN proxy po stronie punktu dystrybucji	✓	–	✓
Pobieranie aktualizacji za pośrednictwem serwerów aktualizacji Kaspersky do repozytoriów punktów dystrybucji, które dystrybuują aktualizacje do zarządzanych urządzeń	✓	– (jeśli co najmniej jedno urządzenie działające pod kontrolą systemu operacyjnego Linux lub macOS znajduje się w zakresie zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji, zadanie zostanie zakończone ze stanem Niepowodzenie nawet wtedy, gdy zostało zakończone pomyślnie na wszystkich urządzeniach z systemem Windows)	✓
Instalowanie aplikacji w trybie push	✓	Ograniczone: nie można przeprowadzić instalacji w trybie push na urządzeniach z systemem Windows przy użyciu punktów dystrybucji systemu macOS.	Ograniczone: nie można przeprowadzić instalacji w trybie push na

			urządzeniach z systemem Windows przy użyciu punktów dystrybucji systemu macOS.
Używanie serwera push	✓	–	✓
Informacje o aplikacjach innych firm			
Zdalne instalowanie aplikacji na urządzeniach	✓	–	–
Aktualizacje oprogramowania	✓	–	–
Konfigurowanie aktualizacji systemu operacyjnego w zasadzie Agenta sieciowego	✓	–	–
Przeglądanie informacji o lukach w oprogramowaniu	✓	–	–
Skanowanie aplikacji w poszukiwaniu luk	✓	–	–
Inwentaryzacja oprogramowania zainstalowanego na urządzeniach	✓	–	–
Maszyny wirtualne			
Instalowanie Agenta sieciowego na maszynie wirtualnej	✓	✓	✓
Ustawienia optymalizacji dla infrastruktury pulpitu wirtualnego (VDI)	✓	✓	✓
Obsługa dynamicznych maszyn wirtualnych	✓	✓	✓
Inne			
Audyt działań na zdalnym urządzeniu klienckim przy użyciu Udostępniania pulpitu Windows	✓	–	–
Monitorowanie stanu ochrony antywirusowej	✓	✓	✓
Zarządzanie ponownymi uruchomieniami urządzenia	✓	–	–
Obsługa przywracania systemu plików	✓	✓	✓
Używanie Agenta sieciowego jako bramy połączenia	✓	✓	✓

Menedżer połączeń	✓	✓	✓
Przełączanie Agenta sieciowego z jednego Serwera administracyjnego na inny (automatycznie według lokalizacji sieciowej)	✓	✓	–
Sprawdzanie połączenia pomiędzy urządzeniem klienckim a Serwerem administracyjnym. Narzędzie klnagchk	✓	✓	✓
Zdalne połączenie z pulpitem urządzenia klienckiego	✓	✓ Korzystając z systemu Virtual Network Computing (VNC).	–
Pobieranie autonomicznego pakietu instalacyjnego poprzez kreator migracji	✓	✓	✓
Przeszukiwanie Zeroconf	–	–	✓

Kaspersky Security Center Web Console

Ta sekcja opisuje działania, które można wykonać przy użyciu Kaspersky Security Center Web Console.

Informacje o Kaspersky Security Center Web Console

Konsola Kaspersky Security Center Web Console (zwana dalej również Kaspersky Security Center Web Console) to aplikacja internetowa przeznaczona do zarządzania stanem systemu bezpieczeństwa sieci chronionej przez aplikacje firmy Kaspersky.

Przy pomocy aplikacji możesz wykonywać następujące czynności:

- Zarządzać stanem systemu ochrony organizacji.
- Instalować aplikacje firmy Kaspersky na urządzeniach w sieci i zarządzać zainstalowanymi aplikacjami.
- Zarządzać profilami utworzonymi dla urządzeń w sieci.
- Zarządzać kontami użytkowników.
- Zarządzać zadaniami dla aplikacji zainstalowanych na urządzeniach w sieci.
- Przeglądać raporty dotyczące stanu systemu ochrony.
- Zarządzać dostarczaniem raportów administratorom systemu i innym specjalistom ds. IT.

Kaspersky Security Center Web Console udostępnia interfejs sieciowy, który zapewnia interakcję między urządzeniem a Serwerem administracyjnym poprzez przeglądarkę internetową. Serwer administracyjny to aplikacja przeznaczona do zarządzania aplikacjami firmy Kaspersky zainstalowanymi na urządzeniach w sieci. Serwer administracyjny nawiązuje połączenie z urządzeniami w sieci poprzez kanały chronione przy pomocy Secure Socket Layer (SSL). Jeśli łączysz się z Kaspersky Security Center Web Console przy użyciu przeglądarki internetowej, przeglądarka nawiąże połączenie z serwerem Kaspersky Security Center Web Console Server.

Kaspersky Security Center Web Console obsługuje się w następujący sposób:

1. Użyj przeglądarki internetowej do nawiązania połączenia z Kaspersky Security Center Web Console, gdzie zostanie wyświetlony interfejs portalu internetowego.
2. Użyj kontrolek portalu internetowego do wybrania polecenia, które chcesz uruchomić. Kaspersky Security Center Web Console wykonuje następujące działania:
    - Jeśli wybrano polecenie używane do pobierania informacji (na przykład wyświetlenie listy urządzeń), Kaspersky Security Center Web Console wyśle do Serwera administracyjnego żądanie informacji, odbierze wymagane dane, a następnie wyśle je do przeglądarki w przejrzystym formacie.
    - Jeśli wybrano polecenie używane do zarządzania (na przykład zdalna instalacja aplikacji), Kaspersky Security Center Web Console odbierze polecenie z przeglądarki i wyśle je do Serwera administracyjnego. W następnej kolejności aplikacja pobierze wynik z Serwera administracyjnego i wyśle go do przeglądarki internetowej w przejrzystym formacie.

Kaspersky Security Center Web Console to wielojęzykowa aplikacja. W każdej chwili możesz zmienić język interfejsu, bez ponownego otwierania aplikacji. Jeśli instalujesz Kaspersky Security Center Web Console wraz z Kaspersky Security Center, Kaspersky Security Center Web Console ma ten sam język interfejsu co plik instalacyjny. Jeśli instalujesz tylko Kaspersky Security Center Web Console, aplikacja ma ten sam język interfejsu co system operacyjny. Jeśli Kaspersky Security Center Web Console nie obsługuje języka pliku instalacyjnego lub systemu operacyjnego, domyślnie jest ustawiany język angielski.

Zarządzanie urządzeniami mobilnymi nie jest obsługiwane w Kaspersky Security Center Web Console. Jednakże, jeśli dodano urządzenia mobilne do grupy administracyjnej przy użyciu konsoli Microsoft Management Console, te urządzenia zostaną także wyświetlone w Kaspersky Security Center Web Console.

Wymagania sprzętowe i programowe Kaspersky Security Center Web Console

Kaspersky Security Center Web Console Server

Minimalne wymagania sprzętowe:

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

Obsługiwane są następujące systemy operacyjne:

- Microsoft Windows (tylko 64-bitowe wersje):
  - Windows Server 2012 Server Core
  - Windows Server 2012 Datacenter
  - Windows Server 2012 Essentials
  - Windows Server 2012 Foundation
  - Windows Server 2012 Standard
  - Windows Server 2012 R2 Server Core
  - Windows Server 2012 R2 Datacenter
  - Windows Server 2012 R2 Essentials
  - Windows Server 2012 R2 Foundation
  - Windows Server 2012 R2 Standard
  - Windows Server 2016 Datacenter (LTSB)
  - Windows Server 2016 Standard (LTSB)
  - Windows Server 2016 Server Core (Opcja instalacji) (LTSB)

- Windows Server 2019 Standard
- Windows Server 2019 Datacenter
- Windows Server 2019 Core
- Windows Server 2022 Standard
- Windows Server 2022 Datacenter
- Windows Server 2022 Core
- Windows Storage Server 2012
- Windows Storage Server 2012 R2
- Windows Storage Server 2016
- Windows Storage Server 2019

- Linux (tylko wersje 64-bitowe):
  - Debian GNU/Linux 9.x (Stretch)
  - Debian GNU/Linux 10.x (Buster)
  - Debian GNU/Linux 11.x (Bullseye)
  - Ubuntu Server 18.04 LTS (Bionic Beaver)
  - Ubuntu Server 20.04 LTS (Focal Fossa)
  - Ubuntu Server 22.04 LTS (Jammy Jellyfish)
  - CentOS 7.x
  - Red Hat Enterprise Linux Server 7.x
  - Red Hat Enterprise Linux Server 8.x
  - Red Hat Enterprise Linux Server 9.x
  - SUSE Linux Enterprise Server 12 (wszystkie pakiety Service Pack)
  - SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack)
  - Astra Linux Special Edition 1.6 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy)
  - Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7.2 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy)
  - Astra Linux Common Edition 2.12
  - Alt Server 9.2
  - Alt Server 10

- Alt 8 SP Server (LKNV.11100-01)
- Alt 8 SP Server (LKNV.11100-02)
- Alt 8 SP Server (LKNV.11100-03)
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition

Maszyna wirtualna oparta na jądrze jest obsługiwana w przypadku następujących systemów operacyjnych zalecanych do wirtualizacji Kaspersky Security Center:

- Alt 8 SP Server (LKNV.11100-01) 64-bitowy
- Alt Server 10 64-bitowy
- Astra Linux Special Edition (Orel, Voronezh, Smolensk) 1.7.2 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy)
- Debian GNU/Linux 11.x (Bullseye) 32-bitowy/64-bitowy
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-bitowy
- RED OS 7.3 Server 64-bitowy
- RED OS 7.3 Certified Edition 64-bitowy

Urządzenia klienckie

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

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

Przeglądarki:

- Mozilla Firefox Extended Support Release w wersji 91.8.0 lub nowszej (91.8.0 wydano 5 kwietnia 2022 r.)
- Google Chrome w wersji 100.0.4896.88 lub nowszej (wersja oficjalna)
- Microsoft Edge w wersji 100 lub nowszej

Diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center Web Console

Rysunek poniżej przedstawia diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center Web Console.

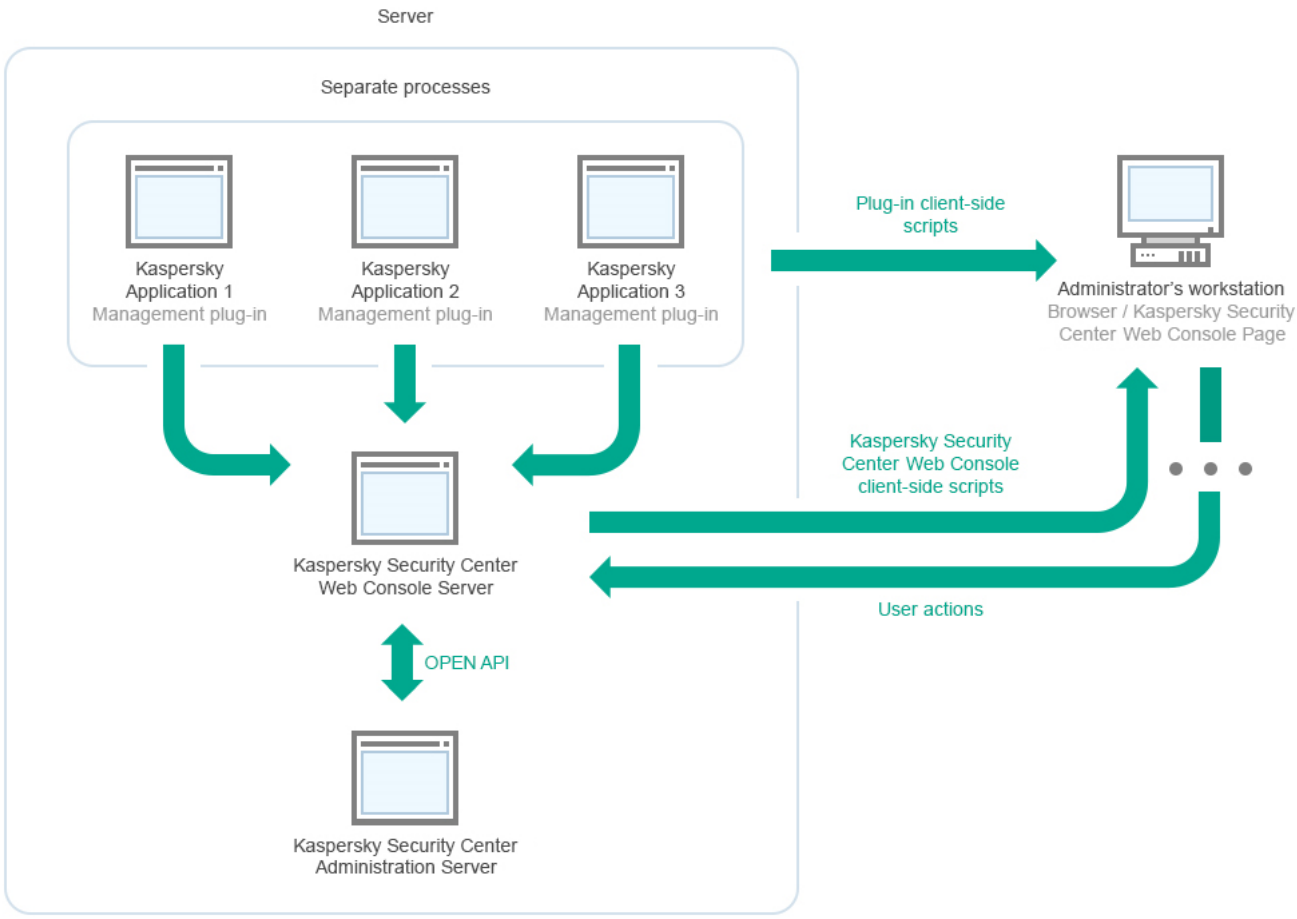


Diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center Web Console

Wtyczki administracyjne dla aplikacji Kaspersky zainstalowanych na chronionych urządzeniach (jedna wtyczka dla każdej aplikacji) są wdrażane razem z Kaspersky Security Center Web Console Server.

Jako administrator uzyskujesz dostęp do Kaspersky Security Center Web Console przy użyciu przeglądarki na swojej stacji roboczej.

Jeśli wykonujesz określone działania w Kaspersky Security Center Web Console, serwer Kaspersky Security Center Web Console Server komunikuje się z serwerem administracyjnym Kaspersky Security Center poprzez interfejs OpenAPI. Serwer Kaspersky Security Center Web Console Server żąda wymaganych informacji z serwera administracyjnego Kaspersky Security Center i wyświetla wyniki Twoich działań w Kaspersky Security Center Web Console.

Porty używane przez Kaspersky Security Center Web Console

W tabeli poniżej przedstawiono porty, które muszą być otwarte na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console Server (zwany również Kaspersky Security Center Web Console).

Porty używane przez Kaspersky Security Center Web Console

Numer portu	Nazwa usługi	Protokół	Przeznaczenie portu	Obs
2001	Wtyczka KSCWebConsolePlugin	HTTPS	Port API używany przez procesy wtyczki zarządzania do odbierania	Uruchami procesów

			żądań z KSCWebConsoleManagementService	node.exe zarządzar
1329, 2003	KSCWebConsoleManagementService	HTTPS	Port API, który jest używany do otrzymywania żądań z usługi KSCWebConsole działającej na tym samym urządzeniu	Aktualizo składnikó Kaspersk Security Web Cor
2005	KSCWebConsole	HTTPS	Port API, który jest używany do otrzymywania żądań z usługi KSCWebConsoleManagementService działającej na tym samym urządzeniu	Uruchami procesów node.exe Kaspersk Security Web Cor
3333	Usługa Kaspersky OSMP KAS	HTTPS	Port punktu końcowego autoryzacji OAuth2.0	Identity a Access M
4004	Usługa Kaspersky OSMP Facade	HTTPS	Port dostawcy tożsamości OAuth2.0	Identity a Access M
4444	Usługa Kaspersky OSMP KAS	HTTPS	Port punktu końcowego introspekcji tokena OAuth2.0	Identity a Access M
8200	—	HTTP	Port API, który jest używany do generowania certyfikatów przy użyciu magazynu HashiCorp Vault (więcej informacji znajdziesz na stronie internetowej HashiCorp Vault)	Instalowa Kaspersk Security Web Cor aktualizov składnikó Kaspersk Security Web Cor
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	Porty API brokera komunikatów, które są używane do komunikacji między procesami Kaspersky Security Center Web Console oraz wtyczek administracyjnych	Interakcja Kaspersk Security Web Cor wtyczek administr

Poniższa tabela zawiera listę portów, które nie muszą być otwarte na urządzeniu, na którym zainstalowano Kaspersky Security Center Web Console Server. Jednak Kaspersky Security Center Web Console używa tych portów dla Identity and Access Manager.

Porty używane przez Kaspersky Security Center Web Console dla Identity and Access Manager

Numer portu	Nazwa usługi	Protokół	Przeznaczenie portu	Obszar
4445	Usługa Kaspersky OSMP KAS	HTTPS	Główny port Identity and Access Manager, który odbiera konfigurację z Kaspersky Security Center Web Console dla portu punktu końcowego autoryzacji OAuth2.0 (więcej informacji na temat OAuth 2.0 można znaleźć na stronie internetowej OAuth)	Identity and Access Manager
2444	Usługa Kaspersky	HTTPS	Port do konfiguracji Identity and Access Manager	Identity and

	OSMP Facade			Access Manager
2445	Usługa Kaspersky OSMP Facade	HTTPS	Port do połączenia Kaspersky OSMP KAS Service z Kaspersky OSMP Facade Service	Identity and Access Manager

Scenariusz: Instalacja i wstępna konfiguracja Kaspersky Security Center Web Console

Ten scenariusz opisuje sposób instalacji Serwera administracyjnego Kaspersky Security Center Kaspersky Security Center Web Console, przeprowadzania wstępnej konfiguracji Serwera administracyjnego przy użyciu kreatora wstępnej konfiguracji, a także instalacji aplikacji Kaspersky na zarządzanych urządzeniach przy użyciu kreatora wdrażania ochrony.

Instalacja i wstępna konfiguracja Kaspersky Security Center Web Console odbywa się w krokach:

1. **Instalowanie systemu zarządzania bazą danych (DBMS)**

   Zainstaluj system DBMS, który będzie używany przez Kaspersky Security Center lub użyj istniejącego systemu.

2. **Instalowanie Serwera administracyjnego, Konsoli administracyjnej, Agenta sieciowego**

   Konsola administracyjna i wersja serwerowa Agenta sieciowego są instalowane wraz z Serwerem administracyjnym.

   Podczas instalacji Serwera administracyjnego Kaspersky Security Center określ, czy chcesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu. Jeśli zdecydujesz się zainstalować oba składniki na tym samym urządzeniu, nie musisz instalować konsoli Kaspersky Security Center Web Console osobno, ponieważ jest ona instalowana automatycznie. Jeśli chcesz zainstalować Kaspersky Security Center Web Console na innym urządzeniu, po zainstalowaniu Serwera administracyjnego Kaspersky Security Center przejdź do instalacji Kaspersky Security Center Web Console.

3. **Instalowanie Kaspersky Security Center Web Console**

   Jeśli nie wybrano instalacji Kaspersky Security Center Web Console wraz z Serwerem administracyjnym Kaspersky Security Center, zainstaluj oddzielnie w pierwszej kolejności Kaspersky Security Center Web Console. Możesz zainstalować Kaspersky Security Center Web Console na innym urządzeniu lub tym samym urządzeniu, na którym zainstalowany jest Serwer administracyjny.

4. **Przeprowadzanie wstępnej konfiguracji**

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

5. **Licencjonowanie Kaspersky Security Center (opcjonalne)**

   Kaspersky Security Center z obsługą podstawowej funkcjonalności Konsoli administracyjnej nie wymaga licencji. Potrzebujesz licencji komercyjnej, jeśli chcesz używać jednej lub kilku dodatkowych funkcji, w tym Zarządzanie lukami i poprawkami, Zarządzanie urządzeniami mobilnymi i Integracja z systemami SIEM. Możesz ręcznie dodać plik klucza lub kod aktywacyjny dla tych funkcji w odpowiednim kroku kreatora wstępnej konfiguracji.

6. **Wyszukiwanie urządzeń w sieci**

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

7. **Rozmieszczanie urządzeń w grupach administracyjnych**

   Ten krok jest częścią kreatora wstępnej konfiguracji, ale możesz także ręcznie przenieść wykryte urządzenia do grup.

8. **Instalowanie Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci**

   Wdrażanie ochrony w sieci firmowej wiąże się z instalacją Agenta sieciowego i aplikacji zabezpieczających (np. Kaspersky Endpoint Security for Windows) na urządzeniach, które zostały wykryte przez Serwer administracyjny podczas wyszukiwania urządzeń.

   Aby zdalnie zainstalować aplikacje, uruchom Kreator wdrażania ochrony.

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

   Przed rozpoczęciem instalacji Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci, upewnij się, że te urządzenia są dostępne (włączone).

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

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

10. **Instalowanie Kaspersky Security for Mobile (opcjonalnie)**

    Jeśli planujesz zarządzać firmowymi urządzeniami mobilnymi, postępuj zgodnie z instrukcjami podanymi w pomocy dla Kaspersky Security for Mobile, aby uzyskać informacje o wdrożeniu Kaspersky Endpoint Security for Android.

11. **Konfigurowanie zasad aplikacji Kaspersky**

    Aby zastosować różne ustawienia aplikacji na różnych urządzeniach, możesz użyć zarządzania ochroną skoncentrowaną na urządzeniu i/lub zarządzania ochroną skoncentrowaną na użytkowniku. Zarządzanie ochroną skoncentrowaną na urządzeniu może zostać zaimplementowane przy użyciu profili i zadań. Możesz zastosować zadania tylko do tych urządzeń, które spełniają określone warunki. Aby ustawić warunki filtrowania urządzeń, użyj znaczników i wyborów urządzeń.

12. **Monitorowanie stanu ochrony sieci**

    Możesz monitorować swoją sieć przy użyciu widżetów na panelu nawigacyjnym, generować raporty z aplikacji Kaspersky, konfigurować i przeglądać wybory zdarzeń otrzymane z aplikacji na zarządzanych urządzeniach, a także przeglądać listy powiadomień.

Instalacja

Ta sekcja opisuje instalację Kaspersky Security Center i Kaspersky Security Center Web Console.

Instalowanie Kaspersky Security Center Web Console

Ta sekcja opisuje sposób oddzielnego zainstalowania serwera Kaspersky Security Center Web Console Server (zwany również Kaspersky Security Center Web Console). Przed instalacją musisz zainstalować system zarządzania bazą danych i Serwerem administracyjnym Kaspersky Security Center. Możesz zainstalować Kaspersky Security Center Web Console na tym samym urządzeniu, na którym jest zainstalowane Kaspersky Security Center, lub na innym.

W celu zainstalowania Kaspersky Security Center Web Console:

1. Z poziomu konta z uprawnieniami administracyjnymi uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe.

   Zostanie uruchomiony kreator instalacji.

2. Wybierz język kreatora instalacji.

3. W oknie powitalnym kliknij **Next**.

   Jeśli Microsoft .NET Framework nie jest zainstalowany, zainstaluj go.

4. W oknie **License Agreement** przeczytaj i zaakceptuj warunki Umowy licencyjnej. Po zaakceptowaniu Umowy licencyjnej instalacja będzie kontynuowana. W innej sytuacji przycisk **Next** będzie niedostępny.

5. W oknie **Destination folder** wybierz folder, w którym zostanie zainstalowana konsola Kaspersky Security Center Web Console (domyślnie, %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Jeżeli taki folder nie istnieje, zostanie utworzony automatycznie w trakcie instalacji.

   Można zmienić folder docelowy przy użyciu przycisku **Browse**.

6. W oknie **Ustawienia połączenia Kaspersky Security Center 14 Web Console** określ następujące informacje:

   - Adres konsoli Kaspersky Security Center Web Console (domyślnie, 127.0.0.1).
   - Port, którego Kaspersky Security Center Web Console będzie używać do połączeń przychodzących, czyli port zapewniający dostęp do konsoli Kaspersky Security Center Web Console z przeglądarki (domyślnie 8080).

   Zalecane jest pozostawienie domyślnych wartości adresu i numeru portu.

   Jeśli chcesz, możesz kliknąć **Test**, aby upewnić się, że wybrany port jest dostępny.

   Jeśli chcesz włączyć zapisywanie działań Kaspersky Security Center Web Console, zaznacz odpowiednią opcję. Jeśli nie zaznaczysz tej opcji, pliki raportu konsoli Kaspersky Security Center Web Console nie zostaną utworzone.

7. W oknie **Account settings** określ nazwy kont i hasła.

   Zalecane jest używanie domyślnych kont.

8. W oknie **Client certificate** wybierz jedną z następujących opcji:

   - **Generate new certificate**. Ta opcja jest zalecana, jeśli nie masz certyfikatu przeglądarki.
   - **Choose existing certificate**. Możesz wybrać tę opcję, jeśli już posiadasz certyfikat przeglądarki; w tym przypadku określ ścieżkę do niego.

Jeśli wybierzesz wygenerowanie nowego certyfikatu, po otwarciu Kaspersky Security Center Web Console przeglądarka może poinformować Cię, że połączenie z Kaspersky Security Center Web Console nie jest prywatne, a certyfikat Kaspersky Security Center Web Console jest nieważny. Takie ostrzeżenie pojawia się, ponieważ certyfikat Kaspersky Security Center Web Console jest certyfikatem z podpisem własnym i jest automatycznie generowany przez Kaspersky Security Center. Aby usunąć to ostrzeżenie, możesz wykonać jedną z następujących czynności:

- Utwórz certyfikat, który jest zaufany w Twojej infrastrukturze i spełnia wymagania certyfikatów niestandardowych. Następnie wybierz opcję **Choose existing certificate** w oknie **Client certificate**, a następnie określ ścieżkę do własnego certyfikatu.

- Zachowaj opcję **Generate new certificate**, a następnie dodaj certyfikat Kaspersky Security Center Web Console do listy zaufanych certyfikatów przeglądarki po zainstalowaniu Kaspersky Security Center Web Console. Zalecamy korzystanie z tej opcji tylko wtedy, gdy nie można utworzyć certyfikatu niestandardowego.

Certyfikaty w formacie PFX nie są obsługiwane przez konsolę Kaspersky Security Center Web Console. Aby użyć takiego certyfikatu, należy najpierw przekonwertować go do obsługiwanego formatu PEM za pomocą narzędzia wieloplatformowego opartego na OpenSSL, takiego jak OpenSSL dla Windows.

9. W oknie **Trusted Administration Servers** upewnij się, że Twój Serwer administracyjny znajduje się na liście, a następnie kliknij **Dalej**, aby przejść do ostatniego okna instalatora.

   Jeśli chcesz dodać nowy Serwer administracyjny do listy, kliknij przycisk **Add**. W otwartym oknie określ właściwości nowego zaufanego Serwera administracyjnego:

   - **Administration Server name**

     Nazwa Serwera administracyjnego, która będzie wyświetlana w oknie logowania Kaspersky Security Center Web Console.

   - **Administration Server address**

     Adres IP urządzenia, na którym instalujesz Serwer administracyjny.

   - **Administration Server port**

     Port OpenAPI, którego Kaspersky Security Center Web Console używa do łączenia się z Serwerem administracyjnym (wartość domyślna to 13299).

   - **Administration Server certificate**

     Plik certyfikatu jest przechowywany na urządzeniu, na którym zainstalowany jest Serwer administracyjny. Domyślna ścieżka do certyfikatu Serwera administracyjnego:

     - W systemie Windows —%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert

     - W systemie Linux — /var/opt/kaspersky/klnagent_srv/1093/cert/

     Jeśli instalujesz Kaspersky Security Center Web Console na tym samym urządzeniu, na którym zainstalowany jest Serwer administracyjny, użyj jednej ze ścieżek podanych powyżej. W przeciwnym razie skopiuj plik certyfikatu z urządzenia, na którym zainstalowany jest Serwer administracyjny, na urządzenie, na którym instalujesz Kaspersky Security Center Web Console, a następnie określ lokalną ścieżkę do certyfikatu.

10. W oknie **Identity and Access Manager (IAM)** określ, czy chcesz zainstalować Identity and Access Manager (zwany również IAM). Jeśli zdecydujesz się zainstalować Identity and Access Manager, określ następujące numery portów:

- **KAS administrator port**. Domyślnie, port 4445 jest używany do odbierania konfiguracji z Kaspersky Security Center Web Console dla portu punktu końcowego autoryzacji OAuth2.0.
- **Facade administrator port**. Domyślnie, port 2444 jest używany do konfiguracji Identity and Access Manager.
- **Facade interaction port**. Domyślnie, port 2445 jest używany do połączenia Kaspersky OSMP KAS Service z Kaspersky OSMP Facade Service.

Jeśli chcesz, możesz zmienić domyślne numery portów. W przyszłości nie będzie można ich zmienić za pomocą Kaspersky Security Center Web Console.

11. W ostatnim oknie instalatora kliknij **Install**, aby rozpocząć instalację.

Po pomyślnym zakończeniu instalacji, skrót pojawi się na Twoim pulpicie i będziesz mógł zalogować się do Kaspersky Security Center Web Console.

Kreator wstępnej konfiguracji Serwera administracyjnego jest uruchamiany, jeśli nie uruchomiono go w Konsoli administracyjnej opartej o konsolę Microsoft Management Console.

Rozwiązywanie problemów

Jeśli konsola Kaspersky Security Center Web Console nie zostanie wyświetlona w przeglądarce pod wpisanym adresem URL:

1. Sprawdź, czy określono poprawną nazwę hosta lub adres IP urządzenia, na którym jest zainstalowana konsola Kaspersky Security Center Web Console.
2. Sprawdź, czy urządzenie, którym chcesz zarządzać, ma dostęp do urządzenia, na którym jest zainstalowana konsola Kaspersky Security Center Web Console.
3. Sprawdź, czy ustawienia zapory sieciowej na urządzeniu, na którym jest zainstalowana konsola Kaspersky Security Center Web Console, zezwala na połączenia przychodzące poprzez port 8080 i dla aplikacji node.exe.
4. W systemie Windows otwórz **Usługi**. Sprawdź, czy usługa Kaspersky Security Center Web Console jest uruchomiona.
5. Sprawdź, czy masz dostęp do Kaspersky Security Center przy użyciu Konsoli administracyjnej.
6. W systemie Windows otwórz **Podgląd zdarzeń**, a następnie wybierz **Dzienniki aplikacji i usług → Dziennik zdarzeń aplikacji Kaspersky**. Upewnij się, że dziennik nie zawiera błędów.

Instalacja Kaspersky Security Center Web Console na platformach Linux

W tej sekcji wyjaśniono sposób instalowania Kaspersky Security Center Web Console Server (zwanego również Kaspersky Security Center Web Console) na urządzeniach działających pod kontrolą systemu operacyjnego Linux (zapoznaj się z listą obsługiwanych dystrybucji Linux).

Instalowanie Kaspersky Security Center Web Console na platformach Linux

W tej sekcji opisano sposób osobnego instalowania Kaspersky Security Center Web Console Server (zwanego również Kaspersky Security Center Web Console) na urządzeniach działających pod kontrolą systemu operacyjnego Linux. Przed instalacją musisz zainstalować system zarządzania bazą danych i Serwerem administracyjnym Kaspersky Security Center.

Użyj jednego z następujących plików instalacyjnych, które odpowiadają dystrybucji Linux zainstalowanej na Twoim urządzeniu:

- Dla Debian — ksc-web-console-[build_number].x86_64.deb
- Dla systemów operacyjnych opartych na RPM — ksc-web-console-[build_number].x86_64.rpm
- Dla Alt 8 SP — ksc-web-console-[build_number]-alt8p.x86_64.rpm

Plik instalacyjny można pobrać ze strony internetowej Kaspersky.

W celu zainstalowania Kaspersky Security Center Web Console:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center Web Console, działa jedna z obsługiwanych dystrybucji systemu Linux.
2. Przeczytaj Umowę licencyjną (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center nie zawiera pliku TXT z treścią umowy EULA, możesz pobrać ten plik ze strony internetowej Kaspersky. Jeśli nie akceptujesz warunków Umowy licencyjnej, nie instaluj aplikacji.
3. Utwórz plik odpowiedzi, który zawiera parametry połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym. Nadaj plikowi nazwę ksc-web-console-setup.json i umieść go w następującym katalogu: /etc/ksc-web-console-setup.json.

   Przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów oraz domyślny adres i port:

   ```
   {
    "address": "127.0.0.1",
    "port": 8080,
    "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
    "acceptEula": true
   }
   ```

   Podczas instalacji konsoli Kaspersky Security Center Web Console w systemie operacyjnym Linux ALT, musisz określić numer portu inny niż 8080, ponieważ port 8080 jest używany przez system operacyjny.

   Kaspersky Security Center Web Console nie można zaktualizować przy użyciu tego samego pliku instalacyjnego .rpm. Jeśli chcesz zmienić ustawienia w pliku odpowiedzi i użyć tego pliku do ponownego zainstalowania aplikacji, w pierwszej kolejności musisz usunąć aplikację, a następnie zainstalować ją ponownie z nowym plikiem odpowiedzi.

4. Z poziomu konta z uprawnieniami administratora użyj wiersza polecenia, aby uruchomić plik instalacji z rozszerzeniem .deb lub .rpm, w zależności od posiadanej dystrybucji systemu Linux.

   - W celu zainstalowania lub uaktualnienia Kaspersky Security Center Web Console z pliku .deb uruchom następujące polecenie:

     ```
     $ sudo dpkg -i ksc-web-console-[build_number].deb
     ```

- W celu zainstalowania Kaspersky Security Center Web Console z pliku .rpm, uruchom następujące polecenie:
  ```
  $ sudo rpm -ivh --nodeps ksc-web-console-[build_number].x86_64.rpm
  ```
- W celu przeprowadzenia aktualizacji z poprzedniej wersji Kaspersky Security Center Web Console, uruchom jedno z następujących poleceń:
  - W przypadku urządzeń z systemem operacyjnym opartym na RPM:
    ```
    $ sudo rpm -Uvh --nodeps --force ksc-web-console-[build_number].x86_64.rpm
    ```
  - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:
    ```
    $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
    ```

Rozpocznie się wypakowywanie pliku instalacji. Zaczekaj na zakończenie instalacji. Kaspersky Security Center Web Console jest instalowany w następującym katalogu: /var/opt/kaspersky/ksc-web-console.

Po zakończeniu instalacji możesz użyć przeglądarki internetowej do otwarcia i zalogowania się do Kaspersky Security Center Web Console.

Parametry instalacji Kaspersky Security Center Web Console

Aby zainstalować Kaspersky Security Center Web Console Server na urządzeniach z systemem Linux, musisz utworzyć plik odpowiedzi w formacie JSON, który zawiera parametry połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym.

Przykład pliku odpowiedzi zawierającego minimalny zestaw parametrów oraz domyślny adres i port:

```
{
 "address": "127.0.0.1",
 "port": 8080,
 "defaultLangId": 1049,
 "enableLog": false,
 "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
 "acceptEula": true,
 "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
 "webConsoleAccount": "Group1:User1",
 "managementServiceAccount": "Group1:User2",
 "serviceWebConsoleAccount": "Group1:User3",
 "pluginAccount": "Group1:User4",
 "messageQueueAccount": "Group1:User5"
}
```

Podczas instalacji konsoli Kaspersky Security Center Web Console w systemie operacyjnym Linux ALT, musisz określić numer portu inny niż 8080, ponieważ port 8080 jest używany przez system operacyjny.

Poniższa tabela opisuje parametry, które mogą zostać określone w pliku odpowiedzi.

Parametry instalacji Kaspersky Security Center Web Console na urządzeniach działających pod kontrolą systemu Linux

Parametr	Opis	Dostępne wa
address	Adres Kaspersky Security Center Web Console Server (wymagany).	Wartość wiersza.

`port`	Numer portu, którego Kaspersky Security Center Web Console Server użyje do nawiązywania połączenia z Serwerem administracyjnym (wymagany).	Wartość numeryczna.
`defaultLangId`	Język interfejsu użytkownika (domyślnie, `1033`).	Kod numeryczny języka: • Niemiecki: `1031` • Angielski: `1033` • Hiszpański: `3082` • Hiszpański (Meksyk): `2058` • Francuski: `1036` • Japoński: `1041` • Kazachstański: `1087` • Polski: `1045` • Portugalski (Brazylia): `1046` • Rosyjski: `1049` • Turecki: `1055` • Chiński uproszczony: `4` • Chiński tradycyjny: `31748` Jeśli nie określono wartości, używany je
`enableLog`	Czy włączyć rejestrowania aktywności Kaspersky Security Center Web Console.	Wartość zerojedynkowa: • `true`—rejestrowanie jest włączone • `false`—rejestrowanie jest wyłączon

`trusted`	Lista zaufanych Serwerów administracyjnych upoważnionych do nawiązywania połączenia z Kaspersky Security Center Web Console (wymagane). Każdy Serwer administracyjny musi być zdefiniowany z następującymi parametrami:
	• Adres Serwera administracyjnego
	• Port OpenAPI, który jest używany przez Kaspersky Security Center Web Console do nawiązywania połączenia z
		Wartość wiersza w następującym form
		`" server address | port | certific`
		Na przykład:
		`"X.X.X.X|13299|/cert/server-1.`
		`1 ||Y.Y.Y.Y|13299|/cert/server-`

	Serwerem administracyjnym (domyślnie jest to port 13299) • Ścieżka do certyfikatu Serwera administracyjnego • Nazwa Serwera administracyjnego, która jest wyświetlana w oknie logowania Parametry są oddzielane pionowymi słupkami. Jeśli określasz kilka Serwerów administracyjnych, oddziel je dwoma pionowymi słupkami.	
`acceptEula`	Czy chcesz zaakceptować warunki Umowy licencyjnej (EULA). Plik zawierający warunki Umowy licencyjnej jest pobierany wraz z plikiem instalacyjnym (wymagane).	Wartość zerojedynkowa: • `true`—W pełni przeczytałem, zrozu Umowy licencyjnej. • `false`—Nie akceptuję postanowień (wybrana domyślnie).
`certDomain`	Jeśli chcesz wygenerować nowy certyfikat, użyj tego parametru do określenia nazwy domeny, dla której zostanie wygenerowany nowy certyfikat.	Wartość wiersza.
`certPath`	Jeśli chcesz użyć istniejącego certyfikatu, użyj tego parametru do określenia ścieżki do pliku certyfikatu.	Wartość wiersza. Określ ścieżkę `„/var/opt/kaspersky/klnagent_s` do korzystania z istniejącego certyfikat niestandardowego określ ścieżkę, w któ certyfikat niestandardowy.
`keyPath`	Jeśli chcesz użyć istniejącego certyfikatu, użyj tego parametru do określenia ścieżki do pliku klucza.	Wartość wiersza.
`webConsoleAccount`	Nazwa konta, pod którym uruchomiona jest usługa KSCWebConsole.	Wartość wiersza w następującym form `name "`. Przykład: `„Grupa1 : Użytkownik1”`. Jeśli nie określono żadnej wartości, inst Center Web Console utworzy nowe ko `user_management_%uid%`.
`managementServiceAccount`	Nazwa konta uprzywilejowanego, w ramach którego uruchomiona jest usługa KSCWebConsoleManagement.	Wartość wiersza w następującym form `name "`. Przykład: `„Grupa1 : Użytkownik1”`. Jeśli nie określono żadnej wartości, inst Center Web Console utworzy nowe ko `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Nazwa konta, w ramach którego uruchomiona jest usługa KSCSvcWebConsole.	Wartość wiersza w następującym form `name "`. Przykład: `„Grupa1 : Użytkownik1”`.

		Jeśli nie określono żadnej wartości, inst Center Web Console utworzy nowe ko `user_svc_nodejs_%uid%`.
`pluginAccount`	Nazwa konta, pod którym uruchomiona jest usługa KSCWebConsolePlugin.	Wartość wiersza w następującym form `name "`. Przykład: „`Grupa1 : Użytkownik1`”. Jeśli nie określono żadnej wartości, inst Center Web Console utworzy nowe ko `user_web_plugin_%uid%`.
`messageQueueAccount`	Nazwa konta, pod którym uruchomiona jest usługa KSCWebConsoleMessageQueue.	Wartość wiersza w następującym form `name "`. Przykład: „`Grupa1 : Użytkownik1`”. Jeśli nie określono żadnej wartości, inst Center Web Console utworzy nowe ko `user_message_queue_%uid%`.

Jeśli określisz parametry `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` lub `messageQueueAccount`, upewnij się, że niestandardowe konta użytkowników należą do tej samej grupy zabezpieczeń. Jeśli te parametry nie zostaną określone, instalator Kaspersky Security Center Web Console utworzy domyślną grupę bezpieczeństwa, a następnie utworzy w tej grupie konta użytkowników o domyślnych nazwach.

Instalowanie Kaspersky Security Center Web Console połączonej z Serwerem administracyjnym zainstalowanym na węzłach klastra przełączania awaryjnego

Ta sekcja opisuje sposób instalacji Serwera Kaspersky Security Center Web Console Server (zwanego dalej także Kaspersky Security Center Web Console), który łączy się z Serwerem administracyjnym zainstalowanym na węzłach klastra pracy awaryjnej Kaspersky lub Microsoft. Przed zainstalowaniem Kaspersky Security Center Web Console zainstaluj system zarządzania bazą danych oraz Serwer administracyjny Kaspersky Security Center na węzłach klastra pracy awaryjnej Kaspersky lub węzłach klastra pracy awaryjnej Microsoft.

Jeśli korzystasz z klastra przełączania awaryjnego firmy Microsoft, nie zalecamy instalowania Kaspersky Security Center Web Console na węźle klastra przełączania awaryjnego. W przypadku awarii węzła utracisz dostęp do Serwera administracyjnego.

Instalowanie Kaspersky Security Center Web Console łączącej się z Serwerem administracyjnym zainstalowanym na węzłach klastra przełączania awaryjnego

1. Wykonaj kroki instalacji Kaspersky Security Center Web Console, zaczynając od kroku 1 do kroku 8.

2. W kroku 9, w oknie **Trusted Administration Servers** kliknij przycisk **Add**, aby dodać klaster przełączania awaryjnego jako zaufany Serwer administracyjny.

   W otwartym oknie określ następujące właściwości:

   - **Administration Server name**

     Nazwa klastra, która będzie wyświetlana w oknie logowania Kaspersky Security Center Web Console.

- **Administration Server address**

  W zależności od typu klastra pracy awaryjnej określ adres klastra:

  - **Klaster trybu failover Kaspersky**. Określ adres IP wirtualnej karty sieciowej jako adres klastra, jeśli karta została utworzona podczas przygotowywania węzłów klastra. W przeciwnym razie określ adres IP modułu równoważenia obciążenia innej firmy, którego używasz.

  - **Klaster pracy awaryjnej firmy Microsoft**. Określ adres klastra uzyskany podczas tworzenia klastra pracy awaryjnej firmy Microsoft.

- **Administration Server port**

  Port OpenAPI, którego Kaspersky Security Center Web Console używa do łączenia się z Serwerem administracyjnym (wartość domyślna to 13299).

- **Administration Server certificate**

  Certyfikat Serwera administracyjnego znajduje się we współdzielonym magazynie danych klastra pracy awaryjnej Kaspersky lub klastra pracy awaryjnej Microsoft. Domyślna ścieżka do pliku certyfikatu: <udostępniony folder danych>\1093\cert\klserver.cer. Skopiuj plik certyfikatu ze współdzielonego magazynu danych na urządzenie, na którym instalujesz Kaspersky Security Center Web Console. Określ lokalną ścieżkę do certyfikatu Serwera administracyjnego.

3. Kontynuuj standardową instalację Kaspersky Security Center Web Console.

Po zakończeniu instalacji, skrót pojawi się na Twoim pulpicie i będziesz mógł/mogła zalogować się do Kaspersky Security Center Web Console.

Jeśli korzystasz z klastra pracy awaryjnej Kaspersky, możesz przejść do opcji **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane** , aby wyświetlić informacje o węzłach klastra i serwerze plików.

Aktualizowanie Kaspersky Security Center Web Console

Jeśli chcesz użyć nowszej wersji Kaspersky Security Center Web Console bez usuwania aktualnie zainstalowanej instancji, możesz użyć standardowej procedury aktualizacji w instalatorze Kaspersky Security Center Web Console.

W celu zaktualizowania Kaspersky Security Center Web Console:

1. Z poziomu konta z uprawnieniami administratora uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe, gdzie <numer kompilacji> oznacza kompilację Kaspersky Security Center Web Console, której numer jest wyższy niż aktualnie zainstalowanej instancji.

2. W otwartym oknie kreatora instalacji wybierz język, a następnie kliknij **OK**.

3. W oknie powitalnym wybierz opcję **Upgrade**, a następnie kliknij **Next**.

4. W oknie **License Agreement** przeczytaj i zaakceptuj warunki Umowy licencyjnej. Po zaakceptowaniu Umowy licencyjnej instalacja będzie kontynuowana. W innej sytuacji przycisk **Next** będzie niedostępny.

5. Przejdź przez kroki kreatora instalacji, aż do zakończenia instalacji. W kolejnych krokach możesz zmodyfikować ustawienia Kaspersky Security Center Web Console, które określiłeś podczas poprzedniej instalacji. W kroku **Ready for Kaspersky Security Center 14 Web Console modification** kliknij przycisk **Upgrade**. Zaczekaj, aż nowe ustawienia zostaną zastosowane, a w kolejnym kroku kreatora instalacji kliknij **Finish**. Możesz także kliknąć odnośnik **Start Kaspersky Security Center 14 Web Console in your browser**, aby od razu uruchomić zaktualizowaną instancję Kaspersky Security Center Web Console.

Modyfikowanie ustawień Kaspersky Security Center Web Console podczas aktualizacji jest dostępne tylko w Kaspersky Security Center Web Console w wersji 12.2 lub nowszej.

Twoja instancja konsoli Kaspersky Security Center Web Console została zaktualizowana.

Certyfikaty do pracy z Kaspersky Security Center Web Console

Ta sekcja opisuje sposób wystawiania i zastępowania certyfikatów dla konsoli Internetowej Kaspersky Security Center Web Console oraz odnawiania certyfikatu dla serwera administracyjnego, jeśli serwer współpracuje z konsolą Internetową Kaspersky Security Center Web Console.

Ponowne wystawianie certyfikatu dla Kaspersky Security Center Web Console

Większość przeglądarek nakłada ograniczenie na okres ważności certyfikatu. Okres ważności certyfikatu Kaspersky Security Center Web Console jest ograniczony do 397 dni, aby mógł się zmieścić w nałożonym ograniczeniu. Możesz zastąpić istniejący certyfikat otrzymany z urzędu certyfikacji, ręcznie publikując nowy certyfikat z podpisem własnym. Możesz ponownie opublikować certyfikat Kaspersky Security Center Web Console, który utracił ważność.

Jeśli już używasz certyfikatu z podpisem własnym, możesz także ponownie opublikować go, aktualizując Kaspersky Security Center Web Console za pośrednictwem standardowej procedury w instalatorze (opcja **Upgrade**).

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

- Określ certyfikat niestandardowy podczas jego ponownego wystawiania (opcja zalecana). Utwórz certyfikat, który jest zaufany w Twojej infrastrukturze i spełnia wymagania certyfikatów niestandardowych.
- Dodaj certyfikat Web Console do listy zaufanych certyfikatów przeglądarki po ponownym wystawieniu certyfikatu. Zalecamy korzystanie z tej opcji tylko wtedy, gdy nie można utworzyć certyfikatu niestandardowego.

W celu publikacji nowego certyfikatu po zainstalowaniu Kaspersky Security Center Web Console po raz pierwszy:

1. Uruchom rutynową instalację Kaspersky Security Center Web Console.
2. W kroku **Client certificate** kreatora instalacji wybierz opcję **Generate new certificate**, a następnie kliknij przycisk **Next**.
3. Przejdź przez pozostałe kroki kreatora instalacji, aż do zakończenia instalacji.

   Nowy certyfikat dla Kaspersky Security Center Web Console jest publikowany z okresem ważności wynoszącym 397 dni.

W celu ponownego opublikowania certyfikatu Kaspersky Security Center Web Console, który utracił ważność:

1. Na koncie z uprawnieniami administratora uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe.

2. W otwartym oknie kreatora instalacji wybierz język, a następnie kliknij **OK**.

3. W oknie powitalnym wybierz opcję **Reissue certificate**, a następnie kliknij **Next**.

4. W następnym kroku zaczekaj, aż ponowna konfiguracja Kaspersky Security Center Web Console zostanie zakończona, a następnie kliknij **Finish**.

   Certyfikat dla Kaspersky Security Center Web Console jest ponownie publikowany dla innego okresu ważności wynoszącego 397 dni.

Jeśli użyjesz Identity and Access Manager, należy również ponownie wystawić wszystkie certyfikaty TLS dla portów, z których korzysta Identity and Access Manager. Kaspersky Security Center Web Console wyświetla powiadomienie po wygaśnięciu certyfikatu. Musisz postępować zgodnie z instrukcjami dotyczącymi powiadomień.

Zastępowanie certyfikatu dla Kaspersky Security Center Web Console

Domyślnie, podczas instalacji Kaspersky Security Center Web Console Server, certyfikat przeglądarki dla aplikacji jest generowany automatycznie. Możesz zastąpić automatycznie wygenerowany certyfikat certyfikatem niestandardowym.

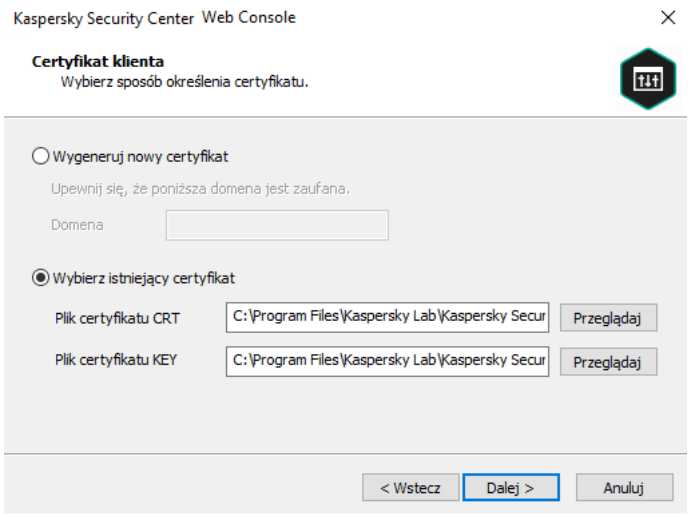
W celu zastąpienia certyfikatu dla Kaspersky Security Center Web Console Server certyfikatem niestandardowym:

1. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console Server, uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe z poziomu konta z uprawnieniami administracyjnymi.

   Zostanie uruchomiony kreator instalacji.

2. W pierwszym kroku kreatora wybierz opcję **Aktualizuj**.

3. W kroku **Certyfikat klienta** wybierz opcję **Wybierz istniejący certyfikat** i określ ścieżkę do certyfikatu niestandardowego.



Określanie certyfikatu klienta

4. W ostatnim kroku kreatora kliknij **Modyfikuj**, aby zastosować nowe ustawienia.

5. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Zakończ**.

Kaspersky Security Center Web Console działa z określonym certyfikatem.

Określanie certyfikatów zaufanych Serwerów administracyjnych w Kaspersky Security Center Web Console

Istniejący certyfikat Serwera administracyjnego jest automatycznie zastępowany nowym przed datą wygaśnięcia certyfikatu. Możesz także zastąpić istniejący certyfikat Serwera administracyjnego innym certyfikatem. Za każdym razem, gdy certyfikat zostanie zmieniony, nowy certyfikat musi zostać określony w ustawieniach Kaspersky Security Center Web Console. W przeciwnym razie Kaspersky Security Center Web Console nie będzie mógł nawiązać połączenia z Serwerem administracyjnym.

Jeśli program Kaspersky Security Center Web Console oraz Serwer administracyjny są zainstalowane na tym samym urządzeniu, Kaspersky Security Center Web Console automatycznie otrzyma nowy certyfikat. Jeśli Kaspersky Security Center Web Console jest zainstalowany na innym urządzeniu, musisz określić lokalną ścieżkę do nowego certyfikatu Serwera administracyjnego.

W celu określenia nowego certyfikatu dla Serwera administracyjnego:

1. Na urządzeniu, na którym jest zainstalowany Serwer administracyjny, skopiuj plik certyfikatu, na przykład, na urządzenie masowego przechowywania.

   Domyślnie, plik certyfikatu jest przechowywany w następującym folderze:

   - W systemie Windows —%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - W systemie Linux — /var/opt/kaspersky/klnagent_srv/1093/cert/

2. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console, umieść plik certyfikatu w folderze lokalnym.

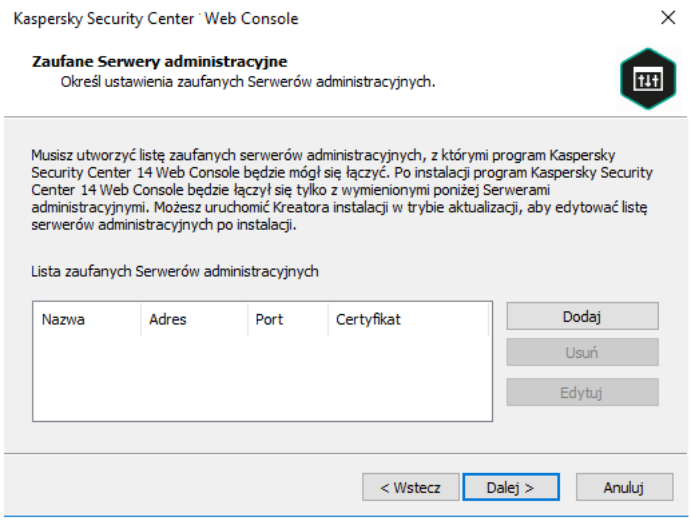
3. Uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe na koncie z uprawnieniami administratora.

   Zostanie uruchomiony kreator instalacji.

4. Na pierwszej stronie kreatora wybierz opcję **Upgrade**.

   Postępuj zgodnie z instrukcjami kreatora.

5. Na stronie **Trusted Administration Servers** wybierz żądany Serwer administracyjny i kliknij przycisk **Edit**.



6. W otwartym oknie **Edit Administration Server** kliknij przycisk **Browse**, określ ścieżkę do pliku nowego certyfikatu, a następnie kliknij przycisk **Update**, aby zastosować zmiany.

7. Na stronie **Gotowy do modyfikacji Kaspersky Security Center Web Console** kreatora kliknij przycisk **Upgrade**, aby rozpocząć aktualizację.

8. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Finish**.

9. Zaloguj się do Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console działa z określonym certyfikatem.

Konwersja certyfikatu PFX do formatu PEM

Aby użyć certyfikatu PFX w Kaspersky Security Center Web Console, musisz najpierw przekonwertować go do formatu PEM za pomocą dowolnego wygodnego narzędzia wieloplatformowego opartego na OpenSSL.

Aby przekonwertować certyfikat PFX do formatu PEM w systemie operacyjnym Windows:

1. W wieloplatformowym narzędziu opartym na OpenSSL wykonaj następujące polecenia:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out server.crt
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes -out key.pem
   ```

   W rezultacie otrzymujesz klucz publiczny jako plik .crt i klucz prywatny jako plik .pem chroniony hasłem.

2. Upewnij się, że pliki .crt i .pem są generowane w tym samym folderze, w którym przechowywany jest plik .pfx.

3. Jeśli plik .crt lub .pem zawiera „Atrybuty worka", usuń te atrybuty za pomocą dowolnego wygodnego edytora tekstu, a następnie zapisz plik.

4. Uruchom ponownie usługę Windows.

5. Kaspersky Security Center Web Console nie obsługuje certyfikatów chronionych hasłem. Dlatego uruchom następujące polecenie w wieloplatformowym narzędziu opartym na OpenSSL, aby usunąć hasło z pliku .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Nie używaj tej samej nazwy dla wejściowych i wyjściowych plików .pem.

   W rezultacie nowy plik .pem jest niezaszyfrowany. Nie musisz wpisywać hasła, aby z niego skorzystać.

Pliki .crt i .pem są gotowe do użycia, więc możesz je określić w instalatorze Kaspersky Security Center Web Console.

Aby przekonwertować certyfikat PFX na format PEM w systemie operacyjnym Linux:

1. W wieloplatformowym narzędziu opartym na OpenSSL wykonaj następujące polecenia:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

```
openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-
END PRIVATE KEY-/p' > key.pem
```

2. Upewnij się, że plik certyfikatu i klucz prywatny są generowane w tym samym katalogu, w którym przechowywany jest plik .pfx.

3. Kaspersky Security Center Web Console nie obsługuje certyfikatów chronionych hasłem. Dlatego uruchom następujące polecenie w wieloplatformowym narzędziu opartym na OpenSSL, aby usunąć hasło z pliku .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Nie używaj tej samej nazwy dla wejściowych i wyjściowych plików .pem.

   W rezultacie nowy plik .pem jest niezaszyfrowany. Nie musisz wpisywać hasła, aby z niego skorzystać.

Pliki .crt i .pem są gotowe do użycia, więc możesz je określić w instalatorze Kaspersky Security Center Web Console.

Migracja do Kaspersky Security Center Linux lub Kaspersky Security Center Cloud Console

Ta sekcja opisuje migrację zarządzanych urządzeń i powiązanych obiektów (polityk, zadań, grup, znaczników i innych obiektów) z Kaspersky Security Center Windows do Kaspersky Security Center Linux lub Kaspersky Security Center Cloud Console.

O migracji do Kaspersky Security Center Cloud Console

Możesz przeprowadzić migrację z Kaspersky Security Center Web Console do Kaspersky Security Center Cloud Console. Następnie uzyskasz dostęp do Serwera administracyjnego i systemu zarządzania bazami danych (DBMS), które są hostowane w infrastrukturze Kaspersky. Nie potrzebujesz fizycznego serwera ani DBMS — oba są utrzymywane przez ekspertów z Kaspersky.

Możesz przeprowadzić migrację zarządzanych urządzeń z systemem operacyjnym Windows, Linux lub macOS pod kontrolą Kaspersky Security Center Cloud Console. Jeśli Twoja sieć zawiera hierarchię Serwerów administracyjnych, możesz ją zapisać w Kaspersky Security Center Cloud Console. Dodatkowo możesz przenieść:

- Zadania i zasady zarządzanych aplikacji
- Zadania globalne
- Niestandardowe wybory urządzeń
- Strukturę grupy administracyjnej i dołączonych urządzeń
- Znaczniki przypisane do przenoszonych urządzeń

Po zakończeniu migracji możesz zarządzać urządzeniami przy użyciu Kaspersky Security Center Cloud Console. Jednocześnie przesłane obiekty są zachowywane, a Agent sieciowy jest ponownie instalowany na wszystkich zarządzanych urządzeniach.

Aby uzyskać informacje na temat przeprowadzania migracji oraz listę wymagań wstępnych, zapoznaj się z *pomocą do Kaspersky Security Center Cloud Console*.

O migracji do Kaspersky Security Center Linux

Ta sekcja zawiera informacje o dostępnych metodach migracji z Kaspersky Security Center Windows do Kaspersky Security Center Linux.

Korzystając z funkcji migracji, możesz przenieść swoje bieżące obiekty (polityki, zadania, grupy, znaczniki i inne obiekty) z Kaspersky Security Center Windows zarządzanego przez Kaspersky Security Center Linux. Aby przenieść pełen zakres obiektów, użyj Kreatora migracji. Kreator ten zapisuje wybrane obiekty w pliku ZIP i umożliwia zaimportowanie obiektów z pliku do Kaspersky Security Center Linux. Oprócz kreatora istnieje inna metoda przesyłania bieżących obiektów, ale ta metoda umożliwia przesyłanie tylko profili i zadań. Możesz przenieść wybrane polityki i zadania za pomocą pliku KLP.

Należy pamiętać, że ta operacja importu poprzez konfigurator migracji nie jest obsługiwana w bieżącej wersji Kaspersky Security Center Linux. Możliwość importowania obiektów zostanie dodana w przyszłych wersjach Kaspersky Security Center Linux. W obecnej wersji możesz migrować określone polityki i zadania.

W aktualnej wersji Kaspersky Security Center Linux możesz przenieść zarządzane urządzenia do zarządzania Kaspersky Security Center Linux przy użyciu narzędzia klmover lub instalując Agenta sieciowego na zarządzanych urządzeniach poprzez zadanie zdalnej instalacji. Zadanie zdalnej instalacji musi być uruchamiane przez punkt dystrybucji oparty na systemie Windows. W tym celu przypisz urządzenie z systemem Windows do działania jako punkt dystrybucji, a następnie włącz opcję **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji** w zadaniu instalacji zdalnej.

Możesz użyć następujących metod migracji zarządzanych urządzeń i danych do Kaspersky Security Center Linux:

- Przeprowadź migrację zarządzanych urządzeń i danych za pomocą kreatora migracji:
  - Migracja bez hierarchii Serwerów administracyjnych

    Wybierz tę opcję, jeśli Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux nie są ułożone w hierarchię. Będziesz musiał przenieść plik eksportu do Kaspersky Security Center Linux na dysk wymienny, pocztą e-mail, poprzez foldery współdzielone lub w inny dogodny sposób. Procesem migracji zarządzasz za pomocą dwóch instancji Kaspersky Security Center Web Console—instancji dla Kaspersky Security Center Windows i drugiej dla Kaspersky Security Center Linux.

  - Migracja z użyciem hierarchii Serwerów administracyjnych

    Wybierz tę opcję, jeśli Serwer administracyjny Kaspersky Security Center Windows działa jako serwer pomocniczy w stosunku do Serwera administracyjnego Kaspersky Security Center Linux. Plik eksportu zostanie automatycznie przesłany do Kaspersky Security Center Linux. Zarządzasz procesem migracji i przełączasz się między serwerami w jednej instancji Kaspersky Security Center Web Console. Jeśli wolisz tę opcję, możesz ustawić Serwery administracyjne w hierarchię, aby uprościć procedurę migracji. W takim przypadku należy wcześniej utworzyć hierarchię przed rozpoczęciem migracji.

- Wyeksportuj określone zadania z Kaspersky Security Center Windows, a następnie zaimportuj zadania do Kaspersky Security Center Linux.

- Wyeksportuj określone profile z Kaspersky Security Center Windows, a następnie zaimportuj profile do Kaspersky Security Center Linux. Powiązane profile zasad są eksportowane i importowane razem z wybranymi politykami.

Migrowanie do Kaspersky Security Center Linux

Ta sekcja opisuje migrację zarządzanych urządzeń i powiązanych obiektów (polityk, zadań, grup, znaczników i innych obiektów) z Kaspersky Security Center Windows Web Console do Kaspersky Security Center Linux, poprzez konfigurator migracji. Możesz włączyć pojedynczą grupę administracyjną do obszaru migracji, aby przywrócić tę samą grupę administracyjną w Kaspersky Security Center Linux. Po zakończeniu migracji wszystkie zarządzane urządzenia i powiązane obiekty będą zarządzane przez Twoją instancję Kaspersky Security Center Linux.

Należy pamiętać, że ta operacja importu poprzez konfigurator migracji nie jest obsługiwana w bieżącej wersji Kaspersky Security Center Linux. Możliwość importowania obiektów zostanie dodana w przyszłych wersjach Kaspersky Security Center Linux. W obecnej wersji możesz migrować określone polityki i zadania.

W bieżącej wersji Kaspersky Security Center Linux możesz przenosić urządzenia zarządzane przez Kaspersky Security Center Linux za pomocą narzędzia klmover lub Agenta sieciowego na zarządzanych urządzeniach poprzez zadanie zdalnej instalacji. Zadanie zdalnej instalacji musi być uruchamiane przez punkt dystrybucji oparty na systemie Windows. W tym celu przypisz urządzenie z systemem Windows do działania jako punkt dystrybucji, a następnie włącz opcję **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji** w zadaniu instalacji zdalnej.

Co możesz migrować

Możesz wyeksportować następujące obiekty:

- Zadania i zasady zarządzanych aplikacji
- Zadania globalne
- Niestandardowe wybory urządzeń
- Strukturę grupy administracyjnej i dołączonych urządzeń
- Znaczniki przypisane do przenoszonych urządzeń

Zanim zaczniesz

Przeczytaj ogólne informacje o migracji do Kaspersky Security Center Linux. Wybierz metodę migracji — używając lub nie używając hierarchii Serwerów administracyjnych Kaspersky Security Center Windows i Kaspersky Security Center Linux.

Kreator migracji

Aby wyeksportować zarządzane urządzenia i powiązane obiekty za pomocą kreatora migracji:

1. W zależności od tego, czy Serwery administracyjne Kaspersky Security Center Windows i Kaspersky Security Center Linux są ułożone w hierarchię, wykonaj jedną z następujących czynności:
   - Jeśli Serwery są ułożone w hierarchię, otwórz Kaspersky Security Center Web Console, a następnie przełącz się do Serwera Kaspersky Security Center Windows.

- Jeśli Serwery nie są ułożone w hierarchię, otwórz Kaspersky Security Center Web Console połączoną z Kaspersky Security Center Windows.

2. W menu głównym przejdź do **Operacje** → **Migracja**.

3. Wybierz **Migracja do Kaspersky Security Center for Linux**, aby uruchomić kreatora i postępować zgodnie z jego instrukcjami.

4. Wybierz grupę administracyjną lub podgrupę do wyeksportowania. Upewnij się, że wybrana grupa lub podgrupa administracyjna zawiera nie więcej niż 10 000 urządzeń.

5. Wybierz zarządzane aplikacje, których zadania i zasady zostaną wyeksportowane. Wybierz tylko te aplikacje, które są obsługiwane przez Kaspersky Security Center Linux. Obiekty nieobsługiwanych aplikacji będą nadal eksportowane, ale nie będą działać.

6. Użyj linków po lewej stronie, aby wybrać zadania globalne, wybrane urządzenia i raporty do wyeksportowania. Łącze **Obiekty grupy** umożliwia wykluczenie niestandardowych ról, użytkowników wewnętrznych i grup zabezpieczeń oraz niestandardowych kategorii aplikacji z eksportu.

7. Plik eksportu (archiwum ZIP) zostanie utworzony i pobrany na komputer.

Logowanie do Kaspersky Security Center Web Console i wylogowywanie

Możesz zalogować się do Kaspersky Security Center Web Console po zainstalowaniu Serwera administracyjnego i serwera Web Console Server. Musisz znać adres internetowy Serwera administracyjnego oraz numer portu określony podczas instalacji (domyślnie jest to port o numerze 8080). W swojej przeglądarce włącz JavaScript.

Możesz zalogować się do Kaspersky Security Center Web Console przy użyciu następujących metod:

- Za pomocą uwierzytelniania domeny

  Jeśli wybierzesz tę metodę, upewnij się, że przeszukiwanie Active Directory zostało aktywowane, a użytkownicy domeny zostali dodani do Serwera administracyjnego.

- Określając nazwę użytkownika i hasło administratora

Logowanie przy użyciu uwierzytelniania domeny

W celu zalogowania się do Kaspersky Security Center Web Console przy użyciu uwierzytelniania domeny:

1. W swojej przeglądarce przejdź do <Adres internetowy Serwera administracyjnego>:<Numer portu>.

   Zostanie wyświetlona strona logowania.

2. Jeśli dodałeś kilka zaufanych serwerów, na liście Serwerów administracyjnych wybierz Serwer administracyjny, z którym chcesz nawiązać połączenie.

   Jeśli dodano tylko jeden Serwer administracyjny, lista Serwery administracyjne nie jest wyświetlana.

3. Wykonaj jedną z poniższych czynności:

   - Kliknij przycisk **Autoryzacja domenowa**.

- Jeżeli jeden lub więcej wirtualnych Serwerów administracyjnych jest utworzonych na Serwerze i chcesz zalogować się do Serwera wirtualnego przy użyciu uwierzytelniania domeny:

  a. Kliknij **Ustawienia zaawansowane**.

  b. Wpisz nazwę wirtualnego Serwera administracyjnego określoną podczas tworzenia wirtualnego Serwera.

  c. Kliknij przycisk **Autoryzacja domenowa**.

Po zalogowaniu, zostanie wyświetlony pulpit nawigacyjny zawierający język i motyw, których ostatnio używałeś. Możesz poruszać się po konsoli Kaspersky Security Center Web Console i użyć jej do pracy z Kaspersky Security Center.

Logowanie poprzez podanie nazwy użytkownika i hasła administratora

W celu zalogowania się do Kaspersky Security Center Web Console poprzez podanie nazwy użytkownika i hasła administratora:

1. W swojej przeglądarce przejdź do <Adres internetowy Serwera administracyjnego>:<Numer portu>.

   Zostanie wyświetlona strona logowania.

2. Jeśli dodałeś kilka zaufanych serwerów, na liście Serwerów administracyjnych wybierz Serwer administracyjny, z którym chcesz nawiązać połączenie.

   Jeśli dodano tylko jeden Serwer administracyjny, lista Serwery administracyjne nie jest wyświetlana.

3. Wykonaj jedną z poniższych czynności:

   - W celu zalogowania się do Serwera administracyjnego:

     a. Wpisz nazwę użytkownika i hasła lokalnego administratora.

     b. Kliknij przycisk **Zaloguj się**.

   - Jeżeli jeden lub więcej wirtualnych Serwerów administracyjnych jest utworzonych na Serwerze i chcesz zalogować się do Serwera wirtualnego:

     a. Kliknij **Ustawienia zaawansowane**.

     b. Wpisz nazwę wirtualnego Serwera administracyjnego określoną podczas tworzenia wirtualnego Serwera.

     c. Wprowadź nazwę użytkownika i hasło administratora, który ma uprawnienia na wirtualnym Serwerze administracyjnym.

     d. Kliknij przycisk **Zaloguj się**.

Po zalogowaniu, zostanie wyświetlony pulpit nawigacyjny zawierający język i motyw, których ostatnio używałeś. Możesz poruszać się po konsoli Kaspersky Security Center Web Console i użyć jej do pracy z Kaspersky Security Center.

Wylogowanie

W celu wylogowania się z Kaspersky Security Center Web Console,

W menu głównym przejdź do ustawień konta i wybierz **Wyloguj się**.

Konsola Kaspersky Security Center Web Console zostanie zamknięta i zostanie wyświetlona strona logowania.

Identity and Access Manager w Kaspersky Security Center Web Console

Ta sekcja zawiera informacje o Identity and Access Manager (nazywanym również IAM).

Informacje o Identity and Access Manager

Identity and Access Manager (nazywany również IAM) to komponent Kaspersky Security Center Web Console, który umożliwia korzystanie z logowania jednokrotnego (SSO) między konsolą Kaspersky Security Center Web Console a interfejsem sieciowym Kaspersky Industrial CyberSecurity for Networks. IAM korzysta z protokołu OAuth 2.0, aby zapewnić autoryzację Kaspersky Industrial CyberSecurity for Networks w Kaspersky Security Center Web Console.

W tym przypadku Kaspersky Industrial CyberSecurity for Networks, do którego uzyskujesz dostęp za pośrednictwem konsoli Kaspersky Security Center Web Console, jest określany jako *serwer zasobów*, a konsola Kaspersky Security Center Web Console i interfejs sieciowy Kaspersky Industrial CyberSecurity for Networks są określane jako *klienty OAuth 2.0*. Serwer zasobów to program, który współpracuje z wieloma użytkownikami i wymaga autoryzacji. Klient używa *tokena* do autoryzacji na serwerze zasobów. Token to unikatowa sekwencja bajtów. Po wygaśnięciu tokena jest on automatycznie ponownie wystawiany. IAM działa jako jeden serwer autoryzacji dla wielu klientów OAuth 2.0.

Możesz zainstalować IAM podczas instalacji Kaspersky Security Center Web Console. Możesz włączyć ją później w dowolnym momencie w ustawieniach Kaspersky Security Center Web Console. Jeśli Kaspersky Industrial CyberSecurity Server lub interfejs webowy Kaspersky Industrial CyberSecurity jest zainstalowany na urządzeniu, który jest zarządzany przez ten sam Serwer administracyjny, IAM wykryje ten program i wyświetli powiadomienie w konsoli Kaspersky Security Center Web Console informujące o tym fakcie. Możesz zarejestrować Kaspersky Industrial CyberSecurity for Networks, a później używać SSO zarówno do konsoli Kaspersky Security Center Web Console, jak i interfejsu sieciowego Kaspersky Industrial CyberSecurity for Networks.

Jeśli wylogujesz się z konsoli Kaspersky Security Center Web Console, Twoja sesja w interfejsie sieciowym Kaspersky Industrial CyberSecurity for Networks zostanie zakończona i wystąpi konieczność ponownego zalogowania się do Kaspersky Security Center Web Console.

Włączanie Identity and Access Manager: scenariusz

Wymagania wstępne

Przed rozpoczęciem upewnij się, że masz dostęp do Kaspersky Industrial CyberSecurity for Networks w wersji 3.1 lub nowszej.

Etapy

Włączenie Identity and Access Manager (zwanego również IAM) przebiega etapami:

1. **Sprawdzanie niezbędnych portów**

   Upewnij się, że porty 3333, 4004 i 4444 są otwarte na urządzeniu, na którym zainstalowano Kaspersky Security Center Web Console. Te porty są potrzebne do korzystania z protokołu OAuth 2.0. Jeśli chcesz, możesz zmienić domyślne numery portów w oknie ustawień Kaspersky Security Center Web Console.

   Oprócz portów 3333, 4004 i 4444, Kaspersky Security Center Web Console używa również portów 4445, 2444 i 2445 do różnych celów.

2. **Instalowanie Identity and Access Manager**

   Podczas instalacji konsoli Kaspersky Security Center Web Console określ, że chcesz zainstalować Identity and Access Manager. Jeśli tego nie zrobiono, uruchom ponownie kreatora instalacji Kaspersky Security Center Web Console.

3. **Konfigurowanie Identity and Access Manager**

   W oknie ustawień Kaspersky Security Center Web Console upewnij się, że przycisk przełącznika **Identity and Access Manager (IAM)** jest włączony. Określ również nazwę DNS urządzenia, na którym zainstalowano Kaspersky Security Center Web Console: aplikacje klienckie nawiążą połączenie z tym urządzeniem.

4. **Określanie ustawień tokena**

   W oknie ustawień Kaspersky Security Center Web Console określ czas życia tokenów i limit czasu autoryzacji, które będą używane przez Identity and Access Manager. Możesz użyć wartości domyślnych lub możesz określić własne wartości zgodnie z własnymi potrzebami.

5. **Przyznawanie certyfikatów**

   Jeśli wolisz korzystać z certyfikatów generowanych przez Serwer administracyjny, to w oknie ustawień Kaspersky Security Center Web Console pobierz certyfikaty główne dla portów używanych przez IAM i roześlij je na stacje robocze użytkowników Kaspersky Security Center Web Console. W przeciwnym razie przeglądarki użytkowników będą wyświetlać komunikaty o błędach podczas próby nawiązania połączenia z konsolą Kaspersky Security Center Web Console.

6. **Rejestrowanie interfejsów webowych Kaspersky Industrial CyberSecurity for Networks Servers i Kaspersky Industrial CyberSecurity for Networks**

   Po zainstalowaniu IAM, konsola Kaspersky Security Center Web Console wyświetla komunikat informujący, że serwer Industrial CyberSecurity for Networks Server (lub kilka serwerów) oraz jeden lub więcej interfejsów webowych Kaspersky Industrial CyberSecurity for Networks czekają na rejestrację. Kliknij tę wiadomość, aby zarejestrować Kaspersky Industrial CyberSecurity for Networks Server (lub kilka serwerów) oraz interfejs webowy (lub kilka interfejsów webowych).

Wyniki

Po zakończeniu tego scenariusza będziesz mógł użyć logowania jednokrotnego i IAM dla Kaspersky Industrial CyberSecurity for Networks i Kaspersky Security Center Web Console.

Konfigurowanie Identity and Access Manager w Kaspersky Security Center Web Console

W celu skonfigurowania Identity and Access Manager zgodnie z własnymi potrzebami:

1. W menu głównym przejdź do sekcji **Ustawienia konsoli** → **Integracja**.
2. W sekcji **Zarządzanie tożsamością i dostępem** upewnij się, że Identity and Access Manager jest włączony.

3. Kliknij odnośnik **Ustawienia**, dostępny w wierszu **Nazwa sieciowa urządzenia Zarządzania tożsamością i dostępem**.

4. Podaj nazwę DNS urządzenia, na którym zainstalowałeś Identity and Access Manager. Aplikacje klienckie będą nawiązywać połączenie z tym urządzeniem.

5. Jeśli chcesz, zmień domyślne ustawienia tokena, ustawienia certyfikatu oraz numery portów, klikając odnośnik **Ustawienia** w odpowiedniej grupie ustawień.

Identity and Access Manager jest włączony i działa zgodnie z Twoimi potrzebami.

Rejestrowanie interfejsu sieciowego Kaspersky Industrial CyberSecurity for Networks w Kaspersky Security Center Web Console

Aby rozpocząć pracę z interfejsem sieciowym Kaspersky Industrial CyberSecurity for Networks za pośrednictwem konsoli Kaspersky Security Center Web Console, musisz najpierw zarejestrować go w konsoli Kaspersky Security Center Web Console.

W celu zarejestrowania interfejsu webowego Kaspersky Industrial CyberSecurity for Networks:

1. Upewnij się, że wykonano następujące czynności:

   - Pobrano i zainstalowano wtyczkę webową Kaspersky Industrial CyberSecurity for Networks.

     Możesz to jednak zrobić później, czekając na synchronizację Kaspersky Industrial CyberSecurity for Networks Server z Serwerem administracyjnym.

   - Ukończyłeś scenariusz przygotowania do użycia technologii jednokrotnego logowania (SSO).

   - Niezbędne ustawienia w interfejsie webowym Kaspersky Industrial CyberSecurity for Networks są określone na stronie Kaspersky Security Center. Aby uzyskać szczegółowe informacje, zapoznaj się z pomocą online do Kaspersky Industrial CyberSecurity for Networks.

   - Jesteś zalogowany w Kaspersky Security Center Web Console na koncie administratora.

   - IAM został skonfigurowany.

2. Przenieś urządzenie, na którym zainstalowano Kaspersky Industrial CyberSecurity for Networks Server, z grupy Urządzenia nieprzypisane do grupy Zarządzane urządzenia:

   a. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane**.

   b. Zaznacz pole wyboru obok urządzenia, na którym jest zainstalowany Kaspersky Industrial CyberSecurity for Networks Server.

   c. Kliknij przycisk **Przenieś do grupy**.

   d. W hierarchii grup administracyjnych zaznacz pole wyboru obok grupy Zarządzane urządzenia.

   e. Kliknij przycisk **Przenieś**.

3. Przejdź do właściwości urządzenia, na którym jest zainstalowany Kaspersky Industrial CyberSecurity for Networks Server.

4. Na stronie właściwości urządzenia, w sekcji **Ogólny** wybierz opcję **Nie odłączaj od Serwera administracyjnego**, a następnie kliknij przycisk **Zapisz**.

5. W oknie właściwości urządzenia wybierz sekcję **Aplikacje**.

6. W sekcji **Aplikacje** wybierz Kaspersky Network Agent.

7. Jeśli aktualny stan aplikacji to *Zatrzymana*, poczekaj, aż zmieni się na *Uruchomiona*.

   Ten proces trwa do 15 minut. Jeśli nie zainstalowałeś jeszcze wtyczki internetowej Kaspersky Industrial CyberSecurity for Networks, możesz to zrobić teraz, podczas oczekiwania.

8. W menu głównym przejdź do sekcji **Ustawienia konsoli** → **Integracja**.

   W polu **Prośby o rejestrację** zostanie wyświetlone jedno oczekujące żądanie.

9. Kliknij odnośnik **Ustawienia** link polem **Prośby o rejestrację**.

10. Na otwartej liście zarejestrowanych klientów zaznacz pole obok nazwy serwera Kaspersky Industrial CyberSecurity for Networks, który ma stan *Oczekuje*, a następnie kliknij przycisk **Zatwierdź**.

    Jeśli nie chcesz rejestrować Kaspersky Industrial CyberSecurity for Networks Server, możesz kliknąć przycisk Odrzuć i wrócić do tej listy później.

    Po kliknięciu przycisku **Zatwierdź**, stan zmieni się na *Zatwierdzony*, a następnie na *Gotowy*. Jeśli stan się nie zmieni, możesz kliknąć przycisk Odśwież.

11. Zamknij listę zarejestrowanych klientów i upewnij się, że wartość w polu **Zarejestrowani klienci** wzrosła.

12. W celu dodania widżetu Kaspersky Industrial CyberSecurity for Networks na pulpicie nawigacyjnym:

    a. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.

    b. Na pulpicie nawigacyjnym kliknij przycisk **Dodaj lub przywróć widżet sieciowy**.

    c. W otwartym menu widżetu wybierz **Inne**.

    d. Wybierz widżet Kaspersky Industrial CyberSecurity for Networks.

    Możesz teraz przejść do interfejsu webowego Kaspersky Industrial CyberSecurity for Networks, korzystając z odnośnika w widżecie.

Po zakończeniu procedury rejestracji, nowy przycisk, **Kaspersky Security Center**, pojawia się na stronie logowania interfejsu webowego Kaspersky Industrial CyberSecurity for Networks. Możesz kliknąć ten przycisk, aby zalogować się do interfejsu webowego Kaspersky Industrial CyberSecurity for Networks przy użyciu danych uwierzytelniających Kaspersky Security Center.

Czas życia tokenów i limit czasu autoryzacji dla Identity and Access Manager

Podczas konfigurowania Identity and Access Manager (zwany również IAM) należy określić ustawienia okresu istnienia tokena i limitu czasu autoryzacji. Ustawienia domyślne mają odzwierciedlać zarówno standardy bezpieczeństwa, jak i obciążenie serwera. Jednakże możesz zmienić te ustawienia zgodnie z zasadami Twojej organizacji.

IAM automatycznie ponownie wystawiają token, gdy zbliża się jego ważność.

Poniższa tabela zawiera domyślne ustawienia okresu istnienia tokena.

Ustawienia czasu życia tokena

Token	Domyślna żywotność (w sekundach)	Opis
Token tożsamości (id_token)	86400	Token tożsamości używany przez klienta OAuth 2.0 (czyli Kaspersky Security Center Web Console lub Kaspersky Industrial CyberSecurity Console). IAM wysyła token identyfikatora zawierający informacje o użytkowniku (czyli profil użytkownika) do klienta.
Token dostępu (access_token)	86400	Token dostępu używany przez klienta OAuth 2.0 do uzyskiwania dostępu do serwera zasobów w imieniu właściciela zasobu zidentyfikowanego przez IAM.
Token odświeżania (refresh_token)	172800	Klient OAuth 2.0 używa tego tokena do ponownego wystawiania tokena tożsamości i tokena dostępu.

Poniższa tabela zawiera listę limitów czasu dla auth_code i login_consent_request.

Ustawienia limitu czasu autoryzacji

Ustawienie	Domyślny limit czasu (w sekundach)	Opis
Kod autoryzacji (auth_code)	3600	Limit czasu wymiany kodu na token. Klient OAuth 2.0 wysyła ten kod do serwera zasobów i otrzymuje w zamian token dostępu.
Przekroczono limit czasu żądania zgody na logowanie (login_consent_request)	3600	Limit czasu na delegowanie uprawnień użytkownika do klienta OAuth 2.0.

Aby uzyskać więcej informacji o tokenach, zajrzyj na stronę internetową OAuth.

Pobieranie i dystrybucja certyfikatów IAM

Domyślnie, Identity and Access Manager używa certyfikatów wygenerowanych przez Serwer administracyjny w celu przyznania przeglądarkom dostępu do Kaspersky Security Center Web Console. Jeśli jednak chcesz, możesz użyć niestandardowych certyfikatów. Niezależnie od używanego certyfikatu, upewnij się, że wszystkie stacje robocze, z których użytkownicy Kaspersky Security Center Web Console uzyskują dostęp do Kaspersky Security Center Web Console, ufają temu certyfikatowi.

W celu pobrania i rozpowszechniania certyfikatów:

1. W menu głównym przejdź do sekcji **Ustawienia konsoli** → **Integracja**.
2. Dla każdego certyfikatu kliknij odnośnik **Ustawienia** w odpowiedniej grupie ustawień, a następnie wykonaj jedną z następujących czynności:
   - Jeśli chcesz użyć certyfikatu wygenerowanego przez Serwer administracyjny podczas instalacji Kaspersky Security Center Web Console:
     1. Wybierz **Certyfikat wygenerowany przez Serwer administracyjny** w otwartym oknie właściwości certyfikatu.

2. Kliknij przycisk **Pobierz**, aby pobrać certyfikat.

3. Roześlij pobrany certyfikat na wszystkie stacje robocze, z których użytkownicy Kaspersky Security Center Web Console uzyskują dostęp do Kaspersky Security Center Web Console.

- Jeśli masz certyfikat, którego chcesz użyć:

  1. Wybierz **Niestandardowy certyfikat TLS** w otwartym oknie właściwości certyfikatu.

  2. Wybierz plik certyfikatu i klucz prywatny.

  3. Kliknij przycisk **OK**.

  4. Roześlij certyfikat do wszystkich stacji roboczych, z których użytkownicy uzyskują dostęp do Kaspersky Security Center Web Console lub Kaspersky Industrial CyberSecurity Console.

Certyfikaty zapewniają użytkownikom dostęp do Kaspersky Security Center Web Console i Kaspersky Industrial CyberSecurity Console.

Musisz ponownie opublikować wszystkie certyfikaty na czas. Certyfikaty wygenerowane przez Serwer administracyjny muszą zostać ponownie wygenerowane ręcznie. Certyfikaty wygenerowane przez instalator Kaspersky Security Center Web Console muszą zostać ponownie wygenerowane przy użyciu instalatora.

Wyłączanie Identity and Access Manager

Jeśli chcesz, możesz wyłączyć Identity and Access Manager (zwany rónież IAM).

W celu wyłączenia IAM:

W oknie ustawień Kaspersky Security Center Web Console ustaw przełącznik IAM na wyłączony.

IAM możesz włączyć w dowolnym momencie później.

Jeżeli aktualizujesz Kaspersky Security Center Web Console za pomocą instalatora i określisz, że nie chcesz instalować IAM, wówczas Kaspersky Security Center Web Console zostanie zaktualizowany, a usługa IAM nie zostanie zainstalowana. Wszystkie informacje dotyczące integracji z Kaspersky Industrial CyberSecurity for Networks zostaną usunięte z komputera, a także pliki konfiguracyjne IAM i pliki dziennika.

Konfigurowanie uwierzytelniania domeny przy użyciu protokołów NTLM i Kerberos

Kaspersky Security Center 14.2 umożliwia korzystanie z uwierzytelniania domeny w OpenAPI przy użyciu protokołów NTLM i Kerberos. Użycie uwierzytelniania domeny umożliwia użytkownikowi systemu Windows włączenie bezpiecznego uwierzytelniania w konsoli Kaspersky Security Center Web Console bez konieczności ponownego wprowadzania hasła w sieci firmowej (technologia pojedynczego logowania).

Uwierzytelnianie domeny w OpenAPI przez protokół Kerberos ma następujące ograniczenia:

- Użytkownik Kaspersky Security Center Web Console musi zostać uwierzytelniony w Active Directory przy użyciu protokołu Kerberos. Użytkownik musi mieć ważny bilet uprawniający do przyznania biletu Kerberos (nazywany również TGT). TGT jest wystawiany automatycznie podczas uwierzytelniania w domenie.

- Musisz skonfigurować uwierzytelnianie Kerberos w przeglądarce. Aby uzyskać szczegółowe informacje, zapoznaj się z dokumentacją używanej przeglądarki.

Jeśli chcesz korzystać z uwierzytelniania domeny przy użyciu protokołów Kerberos, Twoja sieć musi spełniać następujące warunki:

- Serwer administracyjny musi być uruchamiany pod nazwą konta domeny.

- Kaspersky Security Center Web Console Server musi być zainstalowany na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny.

- Musisz określić następujące nazwy główne usługi (SPN) dla konta Serwera administracyjnego:

  - „https/<server.fqnd.name>"

  - „https/<server>"

  <serwer> to nazwa sieciowa urządzenia z Serwerem administracyjnym, a <serwer.fqnd.nazwa> to nazwa FQDN urządzenia z Serwerem administracyjnym.

- Podczas nawiązywania połączenia z Konsolą administracyjną lub konsolą Kaspersky Security Center Web Console, adres Serwera administracyjnego musi być dokładnie taki sam, jak adres, dla którego zarejestrowana jest nazwa główna usługi (SPN). Możesz określić <serverhost.find.name> lub<serverhost>.

- Aby zalogować się bez hasła, proces przeglądarki, w którym konsola Kaspersky Security Center Web Console jest otwarta jako przeglądarka, musi działać na koncie domeny.

Protokoły Kerberos i NTLM są obsługiwane tylko w interfejsie OpenAPI dla Kaspersky Security Center 14.2. Nie są obsługiwane w OpenAPI dla Kaspersky Security Center Linux.

Konfigurowanie Serwera administracyjnego

Ta sekcja opisuje proces konfiguracji i właściwości Serwera administracyjnego Kaspersky Security Center.

Konfigurowanie połączenia Kaspersky Security Center Web Console z Serwerem administracyjnym

W celu określenia portów połączenia Serwera administracyjnego:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty połączenia**.

Aplikacja wyświetli główne ustawienia połączenia wybranego serwera.

Konsola administracyjna jest połączona z Serwerem administracyjnym poprzez port SSL TCP 13291. Ten sam port może być używany przez obiekty automatyzacji klakaut.

Port TCP o numerze 14000 może być używany do podłączania Konsoli administracyjnej, punktów dystrybucji, podrzędnych Serwerów administracyjnych i obiektów narzędzia klakaut, a także do pobierania danych z urządzeń klienckich.

Zazwyczaj, Port TCP o numerze 13000 dla protokołu SSL może być używany tylko przez Agenta sieciowego, podrzędny Serwer administracyjny i główny Serwer administracyjny w DMZ. W niektórych przypadkach konieczne może być podłączenie Konsoli administracyjnej za pośrednictwem portu SSL o numerze 13000:

- Jeśli pojedynczy port SSL będzie używany dla Konsoli administracyjnej i do innych działań (pobierania danych z urządzeń klienckich, podłączania punktów dystrybucji lub podłączania podrzędnych Serwerów administracyjnych).
- Jeśli obiekt narzędzia klakaut nie jest podłączany bezpośrednio do Serwera administracyjnego, ale za pośrednictwem punktu dystrybucji w DMZ.

Przeglądanie raportów połączeń z Serwerem administracyjnym

Historia połączeń i prób nawiązania połączenia z Serwerem administracyjnym podczas jego działania może zostać zapisana w pliku raportu. Informacje w pliku umożliwiają śledzenie nie tylko połączeń w obrębie infrastruktury sieci, ale także nieautoryzowanych prób uzyskania dostępu do serwera.

W celu zapisania zdarzeń nawiązania połączenia z Serwerem administracyjnym:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty połączenia**.

3. Włącz opcję **Zapisuj zdarzenia połączenia z Serwerem administracyjnym**.

Wszystkie dalsze zdarzenia przychodzących połączeń z Serwerem administracyjnym, wyniki autoryzacji i błędy SSL zostaną zapisane do pliku %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Konfigurowanie ustawień dostępu do Internetu dla Serwera administracyjnego

Należy skonfigurować dostęp do Internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji Kaspersky.

Aby określić ustawienia dostępu do Internetu dla Serwera administracyjnego:

1. W menu aplikacji kliknij ikonę ustawień ( ) obok nazwy Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Konfiguracja dostępu do internetu**.

3. Włącz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest włączona, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

   - **Adres**

     Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

   - **Numer portu**

     Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

   - **Pomiń serwer proxy dla adresów lokalnych**

     Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

   - **Uwierzytelnianie na serwerze proxy**

     Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

     To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

   - **Nazwa użytkownika**

     Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

   - **Hasło**

     Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

     Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Dostęp do Internetu można również skonfigurować za pomocą kreatora wstępnej konfiguracji.

Określanie maksymalnej liczby zdarzeń w repozytorium zdarzeń

W sekcji **Repozytorium zdarzeń** okna właściwości Serwera administracyjnego możesz zmodyfikować ustawienia przechowywania zdarzeń w bazie danych Serwera administracyjnego, ograniczając liczbę wpisów zdarzeń i czas przechowywania wpisów. Jeśli określisz maksymalną liczbę zdarzeń, aplikacja oblicza przybliżoną ilość miejsca przechowywania, wymaganą dla określonej liczby. Możesz użyć tego przybliżonego obliczenia do oszacowania wystarczającej ilości wolnego miejsca na dysku, aby uniknąć przepełnienia bazy danych. Domyślna pojemność bazy danych Serwera administracyjnego wynosi 400 000 zdarzeń. Maksymalną dozwoloną pojemnością bazy danych jest 45 milionów zdarzeń.

Jeśli liczba zdarzeń w bazie danych osiągnie maksymalną wartość określoną przez administratora, aplikacja usunie najstarsze zdarzenia i zastąpi je nowymi. Jeśli Serwer administracyjny usuwa starsze zdarzenia, nie może zapisywać nowych zdarzeń do bazy danych. W tym czasie informacje o odrzuconych zdarzeniach są zapisywane w dzienniku zdarzeń aplikacji Kaspersky. Nowe zdarzenia zostają zakolejkowane, a następnie zapisane do bazy danych po zakończeniu operacji usuwania.

Aby ograniczyć liczbę zdarzeń, które mogą być przechowywane w repozytorium zdarzeń na Serwerze administracyjnym:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Repozytorium zdarzeń**. Określ maksymalną liczbę zdarzeń przechowywanych w bazie danych.

3. Kliknij przycisk **Zapisz**.

Dodatkowo możesz zmienić ustawienia dowolnego zadania, aby zapisywać zdarzenia związane z postępem zadania lub zapisywać tylko wyniki wykonania zadania. Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Ustawienia połączenia urządzeń chronionych UEFI

Urządzenie chronione UEFI to urządzenia z programem Kaspersky Anti-Virus dla UEFI zintegrowanym na poziomie BIOS-u. Zintegrowana ochrona zapewnia bezpieczeństwo urządzenia od momentu uruchomienia systemu, natomiast ochrona na urządzeniach bez zintegrowanego oprogramowania zaczyna działać dopiero po uruchomieniu aplikacji zabezpieczającej. Kaspersky Security Center obsługuje zarządzanie tymi urządzeniami.

W celu zmodyfikowania ustawień połączenia urządzeń chronionych UEFI:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty dodatkowe**.

3. Zmodyfikuj odpowiednie ustawienia:

   - **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

     Urządzenia chronione UEFI mogą nawiązywać połączenie z Serwerem administracyjnym.

   - **Port dla urządzeń chronionych UEFI i urządzeń KasperskyOS**

     Możesz zmienić numer portu, jeśli opcja **Otwórz port dla urządzeń chronionych UEFI i urządzeń KasperskyOS** jest włączona. Domyślny numer portu to 13294.

4. Kliknij przycisk **Zapisz**.

Urządzenia chronione UEFI mogą teraz nawiązywać połączenie z Serwerem administracyjnym.

Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego

Dodawanie podrzędnego Serwera administracyjnego (wykonywane na przyszłym głównym Serwerze administracyjnym)

Możesz dodać Serwer administracyjny jako podrzędny Serwer administracyjny, a tym samym utworzyć hierarchię „główny/podrzędny".

W celu dodania podrzędnego Serwera administracyjnego, który jest dostępny do połączenia poprzez Kaspersky Security Center Web Console:

1. Upewnij się, że port 13000 przyszłego głównego Serwera administracyjnego jest dostępny do odbierania połączeń od podrzędnych Serwerów administracyjnych.
2. Na przyszłym głównym Serwerze administracyjnym kliknij ikonę ustawienia ( ).
3. W otwartym oknie właściwości wybierz zakładkę **Serwery administracyjne**.
4. Zaznacz pole obok nazwy grupy administracyjnej, do której chcesz dodać Serwer administracyjny.
5. W wierszu menu kliknij **Połącz podrzędny Serwer administracyjny**.

   Zostanie uruchomiony Kreator dodawania podrzędnego Serwera administracyjnego.
6. W pierwszym kroku kreatora wypełnij następujące pola:

   - **Wyświetlana nazwa podrzędnego Serwera administracyjnego**

     Nazwa, pod którą podrzędny Serwer administracyjny będzie wyświetlany w hierarchii. Jeśli chcesz, możesz wprowadzić adres IP jako nazwę lub możesz użyć nazwy, na przykład „Serwer podrzędny dla grupy 1".

   - **Adres podrzędnego Serwera administracyjnego (opcjonalnie)**

     Określ adres IP lub nazwę domeny podrzędnego Serwera administracyjnego.

   - **Port SSL Serwera administracyjnego**

     Określ numer portu SSL na głównym Serwerze administracyjnym. Domyślny numer portu to 13000.

   - **Port API Serwera administracyjnego**

     Określ numer portu na głównym Serwerze administracyjnym do odbierania połączeń poprzez OpenAPI. Domyślny numer portu to 13299.

   - **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**

Wybierz tę opcję, jeśli podrzędny Serwer administracyjny znajduje się w strefie zdemilitaryzowanej (DMZ).

Jeżeli ta opcja jest zaznaczona, podstawowy Serwer administracyjny inicjuje połączenie z pomocniczym Serwerem administracyjnym. W przeciwnym razie pomocniczy Serwer administracyjny inicjuje połączenie z podstawowym Serwerem administracyjnym.

7. Określ ustawienia połączenia:

   - Wprowadź adres przyszłego podstawowego Serwera administracyjnego.
   - Jeśli przyszły pomocniczy Serwer administracyjny będzie korzystał z serwera proxy, wprowadź adres serwera proxy i poświadczenia użytkownika, aby połączyć się z serwerem proxy.

8. Wprowadź poświadczenia użytkownika, który ma prawa dostępu na przyszłym pomocniczym Serwerze administracyjnym.

   Upewnij się, że weryfikacja dwuetapowa jest wyłączona dla określonego konta. Jeśli dla tego konta włączona jest weryfikacja dwuetapowa, możesz utworzyć hierarchię tylko z przyszłego serwera pomocniczego (zobacz instrukcje poniżej). To znany problem.

   Jeśli ustawienia połączenia są prawidłowe, nawiązywane jest połączenie z przyszłym serwerem pomocniczym i budowana jest hierarchia „primary/secondary". Jeśli połączenie nie powiodło się, sprawdź ustawienia połączenia lub ręcznie określ certyfikat przyszłego Serwera pomocniczego.

   Połączenie może się również nie powieść, ponieważ przyszły serwer pomocniczy jest uwierzytelniany za pomocą samopodpisanego certyfikatu, który został automatycznie wygenerowany przez Kaspersky Security Center. W rezultacie przeglądarka może zablokować pobieranie automatycznie podpisanego certyfikatu. W takim przypadku możesz wykonać jedną z następujących czynności:

   - Dla przyszłego serwera pomocniczego utwórz certyfikat zaufany w Twojej infrastrukturze i spełniający wymagania dotyczące certyfikatów niestandardowych.
   - Dodaj automatycznie podpisany certyfikat przyszłego serwera pomocniczego do listy zaufanych certyfikatów przeglądarki. Zalecamy korzystanie z tej opcji tylko wtedy, gdy nie można utworzyć certyfikatu niestandardowego. Informacje na temat dodawania certyfikatu do listy zaufanych certyfikatów znajdziesz w dokumentacji swojej przeglądarki.

   Połączenie między głównym i pomocniczym Serwerem administracyjnym jest nawiązywane przez port 13000. Zostaną pobrane i zastosowane zadania i zasady z głównego Serwera administracyjnego. Podrzędny Serwer administracyjny jest wyświetlany na głównym Serwerze administracyjnym w grupie administracyjnej, do której został dodany.

Dodawanie podrzędnego Serwera administracyjnego (wykonywane na przyszłym podrzędnym Serwerze administracyjnym)

Jeśli nie udało się nawiązać połączenia z przyszłym podrzędnym Serwerem administracyjnym (na przykład był tymczasowo odłączony lub niedostępny), wciąż możesz dodać podrzędny Serwer administracyjny.

W celu dodania podrzędnego Serwera administracyjnego, który nie jest dostępny do połączenia poprzez Kaspersky Security Center Web Console:

1. Wyślij plik certyfikatu przyszłego głównego Serwera administracyjnego do administratora systemu biura, w którym znajduje się przyszły podrzędny Serwer administracyjny (możesz, na przykład, zapisać plik na urządzeniu zewnętrznym, takim jak dysk flash, lub wysłać go przez pocztę e-mail).

   Plik certyfikatu znajduje się na przyszłym głównym Serwerze administracyjnym w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Poproś administratora systemu zarządzającego przyszłym podrzędnym Serwerem administracyjnym o wykonanie następujących czynności:

   a. Kliknij ikonę ustawienia ( ).

   b. W otwartym oknie właściwości przejdź do sekcji **Hierarchia Serwerów administracyjnych** zakładki **Ogólne**.

   c. Wybierz opcję **Ten Serwer administracyjny jest podrzędnym w hierarchii**.

   d. W polu **Adres głównego Serwera administracyjnego** wprowadź nazwę sieci przyszłego głównego Serwera administracyjnego.

   e. Wybierz wcześniej zapisany plik z certyfikatem przyszłego głównego Serwera administracyjnego, klikając **Przeglądaj**.

   f. Jeśli to konieczne, zaznacz pole **Połącz główny Serwer administracyjny z podrzędnym Serwerem administracyjnym w DMZ**.

   g. Jeśli połączenie z przyszłym podrzędnym Serwerem administracyjnym odbywa się poprzez serwer proxy, wybierz opcję **Użyj serwera proxy** i określ ustawienia połączenia.

   h. Kliknij **Zapisz**.

Zostanie utworzona hierarchia „główny/podrzędny". Główny Serwer administracyjny rozpocznie odbieranie połączenia od podrzędnego Serwera administracyjnego za pośrednictwem portu 13000. Zostaną pobrane i zastosowane zadania i zasady z głównego Serwera administracyjnego. Podrzędny Serwer administracyjny jest wyświetlany na głównym Serwerze administracyjnym w grupie administracyjnej, do której został dodany.

Przeglądanie listy podrzędnych Serwerów administracyjnych

W celu przejrzenia listy podrzędnych (w tym wirtualnych) Serwerów administracyjnych:

W oknie głównym aplikacji kliknij nazwę Serwera administracyjnego, która znajduje się obok ikony ustawienia ( ).

Zostanie wyświetlona lista rozwijana podrzędnych (w tym wirtualnych) Serwerów administracyjnych.

Możesz przejść do dowolnego z tych Serwerów administracyjnych, klikając jego nazwę.

Grupy administracyjne są także wyświetlane, ale są wyszarzone i nie są dostępne do zarządzania w tym menu.

Jeżeli jesteś połączony(-a) z głównym Serwerem administracyjnym w Kaspersky Security Center Web Console i nie możesz połączyć się z wirtualnym Serwerem administracyjnym zarządzanym przez dodatkowy Serwer administracyjny, możesz skorzystać z jednego z następujących sposobów:

- Zmodyfikuj istniejącą instalację Kaspersky Security Center Web Console, aby dodać serwer pomocniczy do listy zaufanych Serwerów administracyjnych. Następnie będzie można połączyć się z wirtualnym Serwerem administracyjnym w Kaspersky Security Center Web Console.

  1. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe z poziomu konta z uprawnieniami administracyjnymi.
  2. Uruchomi się Kreator konfiguracji.
  3. W pierwszym kroku kreatora wybierz opcję **Aktualizuj**.
  4. Na stronie **Modification type** wybierz opcję **Edycja ustawień połączenia**.
  5. Na stronie **Trusted Administration Servers** dodaj wymagany dodatkowy serwer administracyjny.
  6. W ostatnim kroku kreatora kliknij **Modyfikuj**, aby zastosować nowe ustawienia.
  7. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Zakończ**.

- Użyj Kaspersky Security Center Web Console, aby połączyć się bezpośrednio z podrzędnym serwerem administracyjnym, na którym utworzono wirtualny serwer. Następnie będzie można przełączyć się na wirtualny Serwer administracyjny w Kaspersky Security Center Web Console.

- Użyj konsoli administracyjnej opartej na programie MMC, aby połączyć się bezpośrednio z serwerem wirtualnym.

Usuwanie hierarchii Serwerów administracyjnych

Jeśli nie chcesz mieć hierarchii Serwerów administracyjnych, możesz odłączyć je od tej hierarchii.

W celu usunięcia hierarchii Serwerów administracyjnych:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy głównego Serwera administracyjnego.
2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.
3. W grupie administracyjnej, z której chcesz usunąć podrzędny Serwer administracyjny, wybierz podrzędny Serwer administracyjny.
4. W wierszu menu kliknij **Usuń**.
5. W otwartym oknie kliknij **OK**, aby potwierdzić chęć usunięcia podrzędnego Serwera administracyjnego.

Poprzedni główny Serwer administracyjny i poprzedni podrzędny Serwer administracyjny są teraz od siebie niezależne. Hierarchia już nie istnieje.

Konserwacja Serwera administracyjnego

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

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

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

Zadanie Konserwacja Serwera administracyjnego nie obsługuje systemu MariaDB. Jeśli ten system DBMS jest używany w Twojej sieci, administratorzy będą musieli samodzielnie utrzymywać MariaDB.

Zadanie Konserwacja Serwera administracyjnego jest tworzone automatycznie podczas instalacji Kaspersky Security Center. Jeżeli zadanie Konserwacja Serwera administracyjnego zostało usunięte, możesz je utworzyć ręcznie.

W celu utworzenia zadania Konserwacja Serwera administracyjnego:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W oknie Kreatora **Nowe zadanie** wybierz **Konserwacja Serwera administracyjnego** jako typ zadania i kliknij przycisk **Dalej**.
4. Wykonaj pozostałe instrukcje kreatora.

Nowo utworzone zadanie będzie wyświetlane na liście zadań. Dla jednego Serwera administracyjnego można uruchomić tylko jedno zadanie Konserwacja Serwera administracyjnego. Jeśli zadanie Konserwacja Serwera administracyjnego zostało już utworzone dla Serwera administracyjnego, nie będzie można utworzyć nowego zadania Konserwacja Serwera administracyjnego.

Konfigurowanie interfejsu

Możesz skonfigurować interfejs konsoli Kaspersky Security Center Web Console, aby wyświetlał i ukrywał sekcje i elementy interfejsu, w zależności od używanych funkcji.

W celu skonfigurowania interfejsu Kaspersky Security Center Web Console zgodnie z aktualnie używanym zestawem funkcji:

1. W menu głównym przejdź do ustawień konta i wybierz **Opcje interfejsu**.
2. W otwartym oknie **Opcje interfejsu** włącz lub wyłącz wymagane opcje.
3. Kliknij **Zapisz**.

Następnie konsola wyświetla sekcje w menu głównym zgodnie z włączonymi opcjami. Na przykład jeśli włączysz opcję **Pokaż alerty EDR**, w menu głównym pojawi się sekcja **Monitorowanie i raportowanie** → **Alerty**.

Zarządzanie wirtualnymi Serwerami administracyjnymi

W tej sekcji opisano następujące czynności zarządzania wirtualnymi Serwerami administracyjnymi:

- Utwórz wirtualne Serwery administracyjne
- Włącz i wyłącz wirtualny Serwer administracyjny
- Przypisz administratora wirtualnego Serwera administracyjnego
- Zmień Serwer administracyjny dla urządzeń klienckich
- Usuń wirtualne Serwery administracyjne

Tworzenie wirtualnego Serwera administracyjnego

Możesz utworzyć wirtualne Serwery administracyjne i dodać je do grup administracyjnych.

W celu utworzenia i dodania wirtualnego Serwera administracyjnego:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.
2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.
3. Wybierz grupę administracyjną, do której chcesz dodać wirtualny Serwer administracyjny.
   Wirtualny serwer administracyjny będzie zarządzać urządzeniami z wybranej grupy (łącznie z podgrupami).
4. W wierszu menu kliknij **Nowy wirtualny Serwer administracyjny**.
5. W otwartym oknie zdefiniuj właściwości nowego wirtualnego Serwera administracyjnego:
   - **Nazwa wirtualnego Serwera administracyjnego**.
   - **Adres połączenia z Serwerem administracyjnym**
     Możesz określić nazwę lub adres IP serwera administracyjnego.
6. Z listy użytkowników wybierz administratora wirtualnego serwera administracyjnego. Jeśli chcesz, możesz edytować jedno z istniejących kont przed przypisaniem do niego roli administratora lub utworzyć nowe konto użytkownika.
7. Kliknij **Zapisz**.

Nowy wirtualny Serwer administracyjny zostanie utworzony, dodany do grupy administracyjnej i wyświetlony na zakładce **Serwery administracyjne**.

Jeżeli jesteś połączony(-a) z głównym Serwerem administracyjnym w Kaspersky Security Center Web Console i nie możesz połączyć się z wirtualnym Serwerem administracyjnym zarządzanym przez dodatkowy Serwer administracyjny, możesz skorzystać z jednego z następujących sposobów:

- Zmodyfikuj istniejącą instalację Kaspersky Security Center Web Console, aby dodać serwer pomocniczy do listy zaufanych Serwerów administracyjnych. Następnie będzie można połączyć się z wirtualnym Serwerem administracyjnym w Kaspersky Security Center Web Console.

  1. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console uruchom plik instalacyjny ksc-web-console-<numer wersji>.<numer kompilacji>.exe z poziomu konta z uprawnieniami administracyjnymi.
  2. Uruchomi się Kreator konfiguracji.
  3. W pierwszym kroku kreatora wybierz opcję **Aktualizuj**.
  4. Na stronie **Modification type** wybierz opcję **Edycja ustawień połączenia**.
  5. Na stronie **Trusted Administration Servers** dodaj wymagany dodatkowy serwer administracyjny.
  6. W ostatnim kroku kreatora kliknij **Modyfikuj**, aby zastosować nowe ustawienia.
  7. Po pomyślnym zakończeniu ponownej konfiguracji aplikacji, kliknij przycisk **Zakończ**.

- Użyj Kaspersky Security Center Web Console, aby połączyć się bezpośrednio z podrzędnym serwerem administracyjnym, na którym utworzono wirtualny serwer. Następnie będzie można przełączyć się na wirtualny Serwer administracyjny w Kaspersky Security Center Web Console.

- Użyj konsoli administracyjnej opartej na programie MMC, aby połączyć się bezpośrednio z serwerem wirtualnym.

Włączanie i wyłączanie wirtualnego Serwera administracyjnego

Jeśli tworzysz nowy wirtualny Serwer administracyjny, jest on domyślnie włączony. Możesz go wyłączyć lub ponownie włączyć w dowolnym momencie. Wyłączenie lub włączenie wirtualnego Serwera administracyjnego jest równoznaczne z wyłączeniem lub włączeniem fizycznego Serwera administracyjnego.

W celu włączenia lub wyłączenia wirtualnego Serwera administracyjnego:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.
2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.
3. Wybierz wirtualny Serwer administracyjny, który chcesz włączyć lub wyłączyć.
4. W wierszu menu kliknij przycisk **Włącz / wyłącz wirtualny Serwer administracyjny**.

   Stan wirtualnego Serwera administracyjnego jest zmieniany na włączony lub wyłączony, w zależności od jego poprzedniego stanu. Zaktualizowany stan jest wyświetlany obok nazwy Serwera administracyjnego.

Przypisywanie administratora do wirtualnego Serwera administracyjnego

Gdy używasz wirtualnych Serwerów administracyjnych w swojej organizacji, możesz chcieć przypisać dedykowanego administratora dla każdego wirtualnego Serwera administracyjnego. Na przykład, może to być przydatne podczas tworzenia wirtualnych Serwerów administracyjnych do zarządzania oddzielnymi biurami lub działami Twojej organizacji lub jeśli jesteś dostawcą MSP i zarządzasz swoimi dzierżawcami za pośrednictwem wirtualnych Serwerów administracyjnych.

Podczas tworzenia wirtualnego Serwera administracyjnego dziedziczy on listę użytkowników i wszystkie uprawnienia użytkownika podstawowego Serwera administracyjnego. Jeśli użytkownik ma prawa dostępu do Serwera podstawowego, ten użytkownik ma również prawa dostępu do Serwera wirtualnego. Po utworzeniu samodzielnie konfigurujesz prawa dostępu do Serwerów. Jeśli chcesz przypisać administratora tylko do wirtualnego Serwera administracyjnego, upewnij się, że administrator nie ma praw dostępu na podstawowym Serwerze administracyjnym.

Administratora wirtualnego Serwera administracyjnego przypisujesz poprzez nadanie praw dostępu administratora do wirtualnego Serwera administracyjnego. Możesz nadać wymagane prawa dostępu na jeden z następujących sposobów:

- Skonfiguruj ręcznie prawa dostępu administratora
- Przypisz jedną lub więcej ról użytkownika dla administratora

Aby zalogować się do Kaspersky Security Center Web Console, administrator wirtualnego Serwera administracyjnego określa nazwę wirtualnego Serwera administracyjnego, nazwę użytkownika i hasło. Kaspersky Security Center Web Console uwierzytelnia administratora i otwiera wirtualny Serwer administracyjny, do którego administrator ma prawa dostępu. Administrator nie może przełączać się między Serwerami administracyjnymi.

Wymagania wstępne

Przed rozpoczęciem upewnij się, że spełnione są następujące warunki:

- Tworzony jest wirtualny Serwer administracyjny.
- Na głównym Serwerze administracyjnym utworzono konto dla administratora, którego chcesz przypisać do wirtualnego Serwera administracyjnego.
- Masz uprawnienia **Modyfikacja list ACL obiektu** w obszarze funkcjonalnym **Funkcje ogólne** → **Uprawnienia użytkownika**.

Ręczne konfigurowanie praw dostępu

Przypisywanie administratora wirtualnego Serwera administracyjnego:

1. W menu głównym przejdź do wymaganego wirtualnego Serwera administracyjnego:
   a. Kliknij ikonę jodełki (▸) po prawej stronie bieżącej nazwy Serwera administracyjnego.
   b. Wybierz wymagany Serwer administracyjny.
2. W menu aplikacji kliknij ikonę ustawienia (🔧) obok nazwy żądanego Serwera administracyjnego.
   Zostanie otwarte okno właściwości Serwera administracyjnego.
3. Na zakładce **Prawa dostępu** kliknij przycisk **Dodaj**.
   Zostanie otwarta ujednolicona lista użytkowników podstawowego Serwera administracyjnego i bieżącego wirtualnego Serwera administracyjnego.

4. Z listy użytkowników wybierz konto administratora, którego chcesz przypisać do wirtualnego Serwera administracyjnego, a następnie kliknij przycisk **OK**.

   Aplikacja dodaje wybranego użytkownika do listy użytkowników na zakładce **Prawa dostępu**.

5. Zaznacz pole wyboru obok dodanego konta, a następnie kliknij przycisk **Prawa dostępu**.

6. Skonfiguruj uprawnienia, jakie będzie miał administrator na wirtualnym Serwerze administracyjnym.

   W celu pomyślnego uwierzytelnienia administrator musi mieć co najmniej następujące uprawnienia:

   - **Odczyt** bezpośrednio w obszarze funkcjonalnym **Funkcje ogólne** → **Podstawowa funkcjonalność**
   - **Odczyt** bezpośrednio w obszarze funkcjonalnym **Funkcje ogólne** → **Wirtualne Serwery administracyjne**

Aplikacja zapisuje zmodyfikowane uprawnienia użytkownika na koncie administratora.

Konfigurowanie praw dostępu poprzez przypisywanie ról użytkownikom

Alternatywnie możesz przyznać prawa dostępu administratorowi wirtualnego Serwera administracyjnego poprzez role użytkownika. Na przykład, może to być przydatne, jeśli chcesz przypisać kilku administratorów do tego samego wirtualnego Serwera administracyjnego. W takim przypadku można przypisać kontom administratorów identyczne role użytkownika (jedną lub więcej) zamiast konfigurować te same uprawnienia użytkownika w odniesieniu do kilku administratorów.

W celu przypisania administratora wirtualnego Serwera administracyjnego poprzez przypisanie ról użytkownika:

1. Na głównym Serwerze administracyjnym utwórz nową rolę użytkownika, a następnie określ wszystkie wymagane prawa dostępu, które musi posiadać administrator na wirtualnym Serwerze administracyjnym. Możesz utworzyć kilka ról, na przykład jeśli chcesz oddzielić dostęp do różnych obszarów funkcjonalnych.

2. W menu głównym przejdź do wymaganego wirtualnego Serwera administracyjnego:

   a. Kliknij ikonę jodełki (›) po prawej stronie bieżącej nazwy Serwera administracyjnego.

   b. Wybierz wymagany Serwer administracyjny.

3. Przypisz nową rolę lub kilka ról do konta administratora.

Aplikacja przypisuje role do konta administratora.

Konfigurowanie praw dostępu na poziomie obiektu

Oprócz przypisywania praw dostępu na poziomie obszaru funkcjonalnego, możesz skonfigurować dostęp do określonych obiektów na wirtualnym Serwerze administracyjnym, na przykład do określonej grupy administracyjnej lub zadania. W tym celu przełącz się na wirtualny Serwer administracyjny, a następnie skonfiguruj prawa dostępu we właściwościach obiektu.

Zmienianie Serwera administracyjnego dla urządzeń klienckich

Można zmienić Serwer administracyjny zarządzający urządzeniami klienckimi na inny, używając zadania **Zmiana Serwera administracyjnego**. Po zakończeniu zadania wybrane urządzenia klienckie zostaną objęte zarządzaniem przez określony Serwer administracyjny. Możesz przełączać zarządzanie urządzeniami pomiędzy następującymi Serwerami administracyjnymi:

- Główny Serwer administracyjny i jeden z jego wirtualnych Serwerów administracyjnych
- Dwa wirtualne Serwery administracyjne tego samego głównego Serwera administracyjnego

W celu zmiany Serwera administracyjnego zarządzającego urządzeniami klienckimi na inny Serwer:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Dla aplikacji Kaspersky Security Center wybierz zadanie **Zmiana Serwera administracyjnego.**
4. Określ nazwę tworzonego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Wybierz Serwer administracyjny, którego chcesz używać do zarządzania wybranymi urządzeniami.
7. Określ ustawienia konta:
   - Konto domyślne

     Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

     Domyślnie opcja ta jest zaznaczona.
   - Określ konto

     Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.
   - Konto

     Konto, z poziomu którego zadanie jest uruchamiane.
   - Hasło

     Hasło do konta, z poziomu którego zadanie będzie uruchamiane.
8. Jeśli na stronie **Zakończ tworzenie zadania** włączysz opcję **Otwórz szczegóły zadania po jego utworzeniu**, możesz zmodyfikować domyślne ustawienia zadania. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

10. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

11. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

12. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

13. Uruchom utworzone zadanie.

Po zakończeniu wykonywania zadania, urządzenia klienckie, dla których zostało ono utworzone, zostaną przekazane Serwerowi administracyjnemu określonemu w ustawieniach zadania.

Usuwanie wirtualnego Serwera administracyjnego

Jeśli usuniesz wirtualny Serwer administracyjny, wszystkie obiekty utworzone na Serwerze administracyjnym, w tym zasady i zadania, również zostaną usunięte. Zarządzane urządzenia z grup administracyjnych, którymi zarządzał wirtualny Serwer administracyjny, zostaną usunięte z grup administracyjnych. Aby przywrócić urządzenia zarządzane przez Kaspersky Security Center, uruchom przeszukiwanie sieci, a następnie przenieś wykryte urządzenia z grupy Urządzenia nieprzypisane do grup administracyjnych.

W celu usunięcia wirtualnego Serwera administracyjnego:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

2. W otwartym oknie przejdź na zakładkę **Serwery administracyjne**.

3. Wybierz wirtualny Serwer administracyjny, który chcesz usunąć.

4. W wierszu menu kliknij **Usuń**.

Wirtualny Serwer administracyjny zostanie usunięty.

Włączanie ochrony konta przed nieautoryzowaną modyfikacją

Możesz włączyć dodatkową opcję ochrony konta użytkownika przed nieautoryzowaną modyfikacją. Jeżeli opcja jest włączona, modyfikowanie ustawień konta użytkownika wymaga autoryzacji przez użytkownika z uprawnieniami do modyfikacji.

W celu włączenia lub wyłączenia ochrony konta przed nieautoryzowaną modyfikacją:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.

2. Kliknij nazwę wewnętrznego konta użytkownika, dla którego chcesz określić ochronę konta przed nieautoryzowaną modyfikacją.

3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Ochrona konta**.

4. Na zakładce **Ochrona konta** wybierz opcję **Poproś o uwierzytelnienie, aby sprawdzić uprawnienia do modyfikowania kont użytkowników**, jeśli chcesz żądać poświadczeń za każdym razem, gdy ustawienia konta są zmieniane lub modyfikowane. W przeciwnym razie wybierz opcję **Zezwalaj użytkownikom na modyfikowanie tego konta bez dodatkowego uwierzytelniania**.

5. Kliknij przycisk **Zapisz**.

Ochrona konta przed nieautoryzowaną modyfikacją jest włączona dla konta użytkownika.

Weryfikacja dwuetapowa

Ta sekcja opisuje sposób korzystania z weryfikacji dwuetapowej do zmniejszenia ryzyka nieautoryzowanego dostępu do Kaspersky Security Center Web Console.

Scenariusz: Konfigurowanie weryfikacji dwuetapowej dla wszystkich użytkowników

W tym scenariuszu opisano sposób włączenia weryfikacji dwuetapowej dla wszystkich użytkowników oraz sposób wykluczenia konta użytkowników z weryfikacji dwuetapowej. Jeśli nie włączyłeś weryfikacji dwuetapowej dla swojego konta przed włączeniem go dla innych użytkowników, aplikacja najpierw otworzy okno umożliwiające włączenie weryfikacji dwuetapowej dla Twojego konta. W tym scenariuszu opisano również sposób włączenia weryfikacji dwuetapowej na swoim koncie.

Jeśli włączyłeś weryfikację dwuetapową na swoim koncie, możesz przejść do etapu włączenia weryfikacji dwuetapowej dla wszystkich użytkowników.

Wymagania wstępne

Zanim zaczniesz:

- Upewnij się, że Twoje konto użytkownika ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** służącym do modyfikacji ustawień zabezpieczeń dla kont innych użytkowników.

- Upewnij się, że inni użytkownicy Serwera administracyjnego zainstalowali aplikację uwierzytelniającą na swoich urządzeniach.

Etapy

Włączenie weryfikacji dwuetapowej dla wszystkich użytkowników przebiega etapami:

1. **Instalowanie aplikacji uwierzytelniającej na urządzeniu**

   Możesz zainstalować aplikację Google Authenticator, Microsoft Authenticator lub dowolną inną aplikację uwierzytelniającą, która obsługuje algorytm jednorazowego hasła czasowego.

2. **Synchronizacja czasu aplikacji uwierzytelniającej z czasem urządzenia, na którym zainstalowany jest Serwer administracyjny**

Upewnij się, że czas ustawiony w aplikacji uwierzytelniającej jest zsynchronizowany z czasem Serwera administracyjnego.

3. **Włączenie weryfikacji dwuetapowej dla Twojego konta i otrzymanie tajnego klucza do Twojego konta**

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Włączanie weryfikacji dwuetapowej na własnym koncie
   - Dla Kaspersky Security Center Web Console: Włączanie weryfikacji dwuetapowej dla własnego konta

   Po włączeniu weryfikacji dwuetapowej na koncie możesz włączyć weryfikację dwuetapową dla wszystkich użytkowników.

4. **Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników**

   Użytkownicy z włączoną weryfikacją dwuetapową muszą jej używać do logowania się do Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników
   - Dla Kaspersky Security Center Web Console: Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników

5. **Edytowanie nazwy wystawcy kodu zabezpieczającego**

   Jeśli masz kilka Serwerów administracyjnych o podobnych nazwach, konieczna może być zmiana nazw wystawców kodów zabezpieczających w celu lepszego rozpoznawania różnych Serwerów administracyjnych.

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Edytowanie nazwy wystawcy kodu zabezpieczającego
   - Dla Kaspersky Security Center Web Console: Edytowanie nazwy wystawcy kodu zabezpieczającego

6. **Z wyłączeniem kont użytkowników, dla których nie musisz włączać weryfikacji dwuetapowej**

   W razie potrzeby możesz wykluczyć użytkowników z weryfikacji dwuetapowej. Użytkownicy z wykluczonymi kontami nie muszą używać weryfikacji dwuetapowej, aby zalogować się do Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna oparta na MMC: Wykluczanie kont z weryfikacji dwuetapowej
   - Dla Kaspersky Security Center Web Console: Wykluczanie kont z weryfikacji dwuetapowej

Wyniki

Po zakończeniu tego scenariusza:

- Weryfikacja dwuetapowa jest włączona na Twoim koncie.
- Weryfikacja dwuetapowa jest włączona dla wszystkich kont użytkowników Serwera administracyjnego, z wyjątkiem kont użytkowników, które zostały wykluczone.

Informacje o weryfikacji dwuetapowej

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

Kod zabezpieczający posiada identyfikator, o którym mowa w *nazwie wystawcy*. Nazwa wystawcy kodu zabezpieczającego jest używana jako identyfikator Serwera administracyjnego w aplikacji uwierzytelniającej. Możesz zmienić nazwę wydawcy kodu zabezpieczającego. Nazwa wystawcy kodu zabezpieczającego ma domyślną wartość, która jest taka sama jak nazwa Serwera administracyjnego. Nazwa wystawcy jest używana jako identyfikator Serwera administracyjnego w aplikacji uwierzytelniającej. Jeśli zmienisz nazwę wystawcy kodu zabezpieczającego, musisz wydać nowy tajny klucz i przekazać go do aplikacji uwierzytelniającej. Kod zabezpieczający jest jednorazowy i ważny do 90 sekund (dokładny czas może się różnić).

Każdy użytkownik, dla którego włączono weryfikację dwuetapową, może ponownie wydać swój własny tajny klucz. Jeśli użytkownik uwierzytelnia się za pomocą ponownie wydanego tajnego klucza i używa go do logowania, Serwer administracyjny zapisuje nowy tajny klucz dla konta użytkownika. Jeśli użytkownik wprowadzi nowy tajny klucz niepoprawnie, Serwer administracyjny nie zapisze nowego tajnego klucza i pozostawi aktualny tajny klucz ważny do dalszej autoryzacji.

Każde oprogramowanie uwierzytelniające, które obsługuje algorytm jednorazowego hasła czasowego (TOTP), może być używane jako aplikacja uwierzytelniająca, na przykład Google Authenticator. Aby wygenerować kod zabezpieczający, musisz zsynchronizować czas ustawiony w aplikacji uwierzytelniającej z czasem ustawionym dla Serwera administracyjnego.

Aplikacja uwierzytelniająca generuje kod zabezpieczający w następujący sposób:

1. Serwer administracyjny generuje specjalny tajny klucz i kod QR.
2. Przekazujesz wygenerowany tajny klucz lub kod QR do aplikacji uwierzytelniającej.
3. Aplikacja uwierzytelniająca generuje jednorazowy kod zabezpieczający, który należy przekazać do okna uwierzytelniania Serwera administracyjnego.

Zdecydowanie zalecamy zainstalowanie aplikacji uwierzytelniającej na więcej niż jednym urządzeniu. Zapisz tajny klucz (lub kod QR) i przechowuj go w bezpiecznym miejscu. Pomoże to w przywróceniu dostępu do Kaspersky Security Center Web Console w przypadku utraty dostępu do urządzenia mobilnego.

Aby zabezpieczyć korzystanie z Kaspersky Security Center, możesz włączyć weryfikację dwuetapową dla swojego konta i włączyć weryfikację dwuetapową dla wszystkich użytkowników.

Możesz wykluczyć konta z weryfikacji dwuetapowej. Może to być konieczne w przypadku kont usług, które nie mogą otrzymać kodu zabezpieczającego dla uwierzytelnienia.

Weryfikacja dwuetapowa działa według następujących zasad:

- Tylko konto użytkownika z uprawnieniem Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** umożliwia weryfikację dwuetapową dla wszystkich użytkowników.
- Tylko użytkownik, który włączył weryfikację dwuetapową na swoim koncie, może włączyć opcję weryfikacji dwuetapowej dla wszystkich użytkowników.
- Tylko użytkownik, który włączył weryfikację dwuetapową na swoim koncie, może wykluczyć inne konta użytkowników z listy weryfikacji dwuetapowej włączonej dla wszystkich użytkowników.
- Użytkownik może włączyć weryfikację dwuetapową tylko dla swojego konta.
- Konto użytkownika, który posiada uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika** i jest zalogowany do Kaspersky Security Center Web Console przy użyciu weryfikacji dwuetapowej, może wyłączyć weryfikację dwuetapową: dla każdego innego użytkownika tylko wtedy, gdy weryfikacja dwuetapowa dla wszystkich użytkowników jest wyłączona, dla użytkownika wykluczonego z listy weryfikacji dwuetapowej, która jest włączona dla wszystkich użytkowników.
- Każdy użytkownik, który zalogował się do Kaspersky Security Center Web Console przy użyciu weryfikacji dwuetapowej, może ponownie wydać swój własny tajny klucz.
- Możesz włączyć opcję weryfikacji dwuetapowej dla wszystkich użytkowników dla Serwera administracyjnego, z którym aktualnie pracujesz. Jeśli włączysz tę opcję na Serwerze administracyjnym, włączysz tę opcję również dla jego kont użytkowników jego wirtualnych Serwerów administracyjnych i nie włączysz weryfikacji dwuetapowej dla kont użytkowników podrzędnych Serwerów administracyjnych.

Jeśli dla konta użytkownika na Serwerze administracyjnym Kaspersky Security Center 13 włączona jest weryfikacja dwuetapowa, użytkownik nie będzie mógł zalogować się do konsoli Kaspersky Security Center Web Console w wersji 12, 12.1 lub 12.2.

Włączanie weryfikacji dwuetapowej dla własnego konta

Użytkownik może włączyć weryfikację dwuetapową tylko dla swojego konta.

Zanim włączysz weryfikację dwuetapową na swoim koncie, upewnij się, że aplikacja uwierzytelniająca jest zainstalowana na Twoim urządzeniu mobilnym. Upewnij się, że czas ustawiony w aplikacji uwierzytelniającej jest zsynchronizowany z czasem ustawionym na urządzeniu, na którym jest zainstalowany Serwer administracyjny.

W celu włączenia weryfikacji dwuetapowej na koncie użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij nazwę swojego konta.
3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Ochrona konta**.
4. Na zakładce **Ochrona konta**:
   a. Wybierz opcję **Zażądaj nazwę użytkownika, hasło i kod zabezpieczający (weryfikacja dwuetapowa)**.
   b. W otwartym oknie weryfikacji dwuetapowej wprowadź tajny klucz w aplikacji uwierzytelniającej lub zeskanuj kod QR i otrzymaj jednorazowy kod zabezpieczający.

Możesz podać tajny klucz w aplikacji uwierzytelniającej ręcznie lub zeskanować kod QR za pomocą urządzenia mobilnego.

c. W oknie weryfikacji dwuetapowej określ kod zabezpieczający, wygenerowany przez aplikację uwierzytelniającą, a następnie kliknij przycisk **Sprawdź i zastosuj**.

5. Kliknij przycisk **Zapisz**.

Weryfikacja dwuetapowa jest włączona na Twoim koncie.

Włączanie weryfikacji dwuetapowej dla wszystkich użytkowników

Możesz włączyć weryfikację dwuetapową dla wszystkich użytkowników Serwera administracyjnego, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów bezpośrednio w obszarze funkcjonalnym **Cechy ogólne: Uprawnienia użytkownika** i jeśli jesteś uwierzytelniony za pomocą weryfikacji dwuetapowej. Jeśli nie włączyłeś weryfikacji dwuetapowej na swoim koncie przed włączeniem jej dla wszystkich użytkowników, aplikacja otworzy okno dla włączenia weryfikacji dwuetapowej dla własnego konta.

W celu włączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości ustaw przycisk przełącznika opcji **weryfikacja dwuetapowa dla wszystkich użytkowników** w pozycji włączenia.

Weryfikacja dwuetapowa jest włączona dla wszystkich użytkowników. Od teraz wszyscy użytkownicy Serwera administracyjnego, w tym użytkownicy dodani po włączeniu weryfikacji dwuetapowej dla wszystkich użytkowników, muszą konfigurować weryfikację dwuetapową dla swoich kont, z wyjątkiem użytkowników, których konta są wykluczone z weryfikacji dwuetapowej.

Wyłączanie weryfikacji dwuetapowej dla konta użytkownika

Możesz wyłączyć weryfikację dwuetapową na swoim koncie, a także na koncie dowolnego innego użytkownika.

Możesz wyłączyć weryfikację dwuetapową konta innego użytkownika, gdy masz uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika**.

W celu wyłączenia weryfikacji dwuetapowej dla konta użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.

2. Kliknij nazwę wewnętrznego konta użytkownika, dla którego chcesz wyłączyć weryfikację dwuetapową. Może to być Twoje własne konto lub konto innego użytkownika.

3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Ochrona konta**.

4. Na zakładce **Ochrona konta** wybierz opcję **Zażądaj tylko nazwę użytkownika i hasło**, jeśli chcesz wyłączyć weryfikację dwuetapową dla konta użytkownika.

5. Kliknij przycisk **Zapisz**.

Weryfikacja dwuetapowa jest wyłączona dla konta użytkownika.

Wyłączanie weryfikacji dwuetapowej dla wszystkich użytkowników

Możesz wyłączyć weryfikację dwuetapową dla wszystkich użytkowników, jeśli weryfikacja dwuetapowa jest włączona dla Twojego konta, a Twoje konto posiada uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika**. Jeśli weryfikacja dwuetapowa nie jest włączona na Twoim koncie, musisz włączyć weryfikację dwuetapową dla swojego konta przed wyłączeniem jej dla wszystkich użytkowników.

W celu wyłączenia weryfikacji dwuetapowej dla wszystkich użytkowników:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości ustaw przycisk przełącznika opcji **weryfikacja dwuetapowa dla wszystkich użytkowników** w pozycji wyłączenia.

3. Wprowadź poświadczenia swojego konta w oknie uwierzytelniania.

Weryfikacja dwuetapowa jest wyłączona dla wszystkich użytkowników.

Wykluczanie kont z weryfikacji dwuetapowej

Możesz wykluczyć konta użytkowników z weryfikacji dwuetapowej, jeśli masz uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika**.

Jeśli konto użytkownika jest wykluczone z listy weryfikacji dwuetapowej dla wszystkich użytkowników, ten użytkownik nie musi korzystać z weryfikacji dwuetapowej.

> Wykluczenie kont z weryfikacji dwuetapowej może być konieczne w przypadku kont usług, które nie mogą przekazać kodu zabezpieczającego podczas uwierzytelniania.

Jeśli chcesz wykluczyć niektóre konta użytkowników z weryfikacji dwuetapowej:

1. W pierwszej kolejności musisz przeprowadzić Przeszukiwanie Active Directory, aby odświeżyć listę użytkowników Serwera administracyjnego, jeśli chcesz wykluczyć konta Active Directory.

2. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

3. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości, w tabeli wykluczeń weryfikacji dwuetapowej kliknij przycisk **Dodaj**.

4. W oknie, które zostanie otwarte:

   a. Wybierz konta użytkowników, które chcesz wykluczyć.

   b. Kliknij przycisk **OK**.

Wybrane konta użytkowników są wykluczone z weryfikacji dwuetapowej.

Generowanie nowego tajnego klucza

Możesz wygenerować nowy tajny klucz do weryfikacji dwuetapowej dla swojego konta tylko wtedy, gdy jesteś autoryzowany za pomocą weryfikacji dwuetapowej.

W celu wygenerowania nowego tajnego klucza dla konta użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij nazwę konta użytkownika, dla którego chcesz wygenerować nowy tajny klucz dla weryfikacji dwuetapowej.
3. W otwartym oknie ustawień użytkownika wybierz zakładkę **Ochrona konta**.
4. Na zakładce **Ochrona konta** kliknij odnośnik **Wygeneruj nowy tajny klucz**.
5. W otwartym oknie weryfikacji dwuetapowej określ nowy klucz zabezpieczeń wygenerowany przez aplikację uwierzytelniającą.
6. Kliknij przycisk **Sprawdź i zastosuj**.

Dla użytkownika jest generowany nowy tajny klucz.

Jeśli zgubisz swoje urządzenie mobilne, możesz zainstalować aplikację uwierzytelniającą na innym urządzeniu mobilnym i wygenerować nowy tajny klucz, aby przywrócić dostęp do Kaspersky Security Center Web Console.

Edytowanie nazwy wystawcy kodu zabezpieczającego

Możesz mieć kilka identyfikatorów (nazywanych wystawcami) dla różnych Serwerów administracyjnych. Możesz zmienić nazwę wystawcy kodu zabezpieczającego w przypadku, gdy, na przykład, jeśli Serwer administracyjny już używa podobnej nazwy wystawcy kodu zabezpieczającego dla innego Serwera administracyjnego. Domyślnie, nazwa wystawcy kodu zabezpieczającego jest taka sama, jak nazwa Serwera administracyjnego.

Po zmianie nazwy wystawcy kodu zabezpieczającego należy ponownie wystawić nowy tajny klucz i przekazać go do aplikacji uwierzytelniającej.

W celu określenia nowej nazwy wystawcy kodu zabezpieczającego:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. W otwartym oknie ustawień użytkownika wybierz zakładkę **Ochrona konta**.

3. Na zakładce **Ochrona konta** kliknij odnośnik **Edytuj**.

   Zostanie otwarta sekcja **Edytuj wydawcę kodu zabezpieczającego**.

4. Określ nową nazwę wydawcy kodu zabezpieczającego.

5. Kliknij przycisk **OK**.

Nowa nazwa wystawcy kodu zabezpieczającego została określona dla Serwera administracyjnego.

Tworzenie kopii zapasowej i przywracanie danych Serwera administracyjnego

Tworzenie kopii zapasowej danych umożliwia przeniesienie Serwera administracyjnego z jednego urządzenia na inne, bez utraty danych. Dzięki kopii zapasowej możesz przywrócić dane podczas przenoszenia bazy danych Serwera administracyjnego na inne urządzenie lub podczas aktualizacji do nowej wersji Kaspersky Security Center.

Pamiętaj, że nie są tworzone kopie zapasowe zainstalowanych wtyczek do zarządzania. Po przywróceniu danych Serwera administracyjnego z kopii zapasowej należy pobrać i ponownie zainstalować wtyczki dla zarządzanych aplikacji.

Możesz utworzyć kopię zapasową danych Serwera administracyjnego w jeden z następujących sposobów:

- Tworząc i uruchamiając zadanie wykonywania kopii zapasowej danych poprzez Konsolę administracyjną.
- Uruchamiając narzędzie klbackup na urządzeniu, na którym jest zainstalowany Serwer administracyjny. To narzędzie znajduje się w pakiecie dystrybucyjnym Kaspersky Security Center. Po zainstalowaniu Serwera administracyjnego, narzędzie jest umieszczane w katalogu głównym folderu docelowego, określonego podczas instalacji aplikacji.

W kopii zapasowej Serwera administracyjnego zapisywane są następujące dane:

- Baza danych Serwera administracyjnego (profile, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym).
- Informacje o konfiguracji struktury grup administracyjnych i urządzeń klienckich.
- Repozytorium pakietów dystrybucyjnych aplikacji przeznaczonych do zdalnego zainstalowania.
- Certyfikat Serwera administracyjnego.

Odzyskanie danych Serwera administracyjnego jest możliwe tylko przy użyciu narzędzia klbackup.

Tworzenie zadania wykonywania kopii zapasowej

Zadania kopii zapasowej są zadaniami Serwera administracyjnego i są tworzone podczas działania kreatora wstępnej konfiguracji. Jeśli zadanie kopii zapasowej utworzone przez Kreator wstępnej konfiguracji zostało usunięte, możesz je utworzyć ręcznie.

W celu utworzenia zadania kopii zapasowej danych Serwera administracyjnego:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W oknie **Nowe zadanie** wybierz typ zadania **Kopia zapasowa danych Serwera administracyjnego**
4. Wykonaj pozostałe instrukcje kreatora.

Zadanie**Kopia zapasowa danych Serwera administracyjnego** może zostać utworzone tylko w jednej kopii. Jeśli dla Serwera administracyjnego już utworzono zadanie tworzenia kopii zapasowych danych Serwera administracyjnego, nie będzie wyświetlane w oknie wyboru typu zadania kreatora tworzenia zadania kopii zapasowej Serwera administracyjnego.

Przenoszenie Serwera administracyjnego na inne urządzenie

Jeśli chcesz użyć Serwera administracyjnego na nowym urządzeniu, możesz je przenieść w jeden z następujących sposobów:

- Przenieś Serwer administracyjny i serwer bazy danych na nowe urządzenie.
- Zachowaj serwer bazy danych na poprzednim urządzeniu i przenieś tylko Serwer administracyjny na nowe urządzenie.

W celu przeniesienia Serwera administracyjnego i serwera bazy danych na nowe urządzenie:

1. Na poprzednim urządzeniu utwórz kopię zapasową danych Serwera administracyjnego.

   W tym celu możesz uruchomić zadanie tworzenia kopii zapasowej danych poprzez Kaspersky Security Center Web Console lub uruchomić narzędzie klbackup.

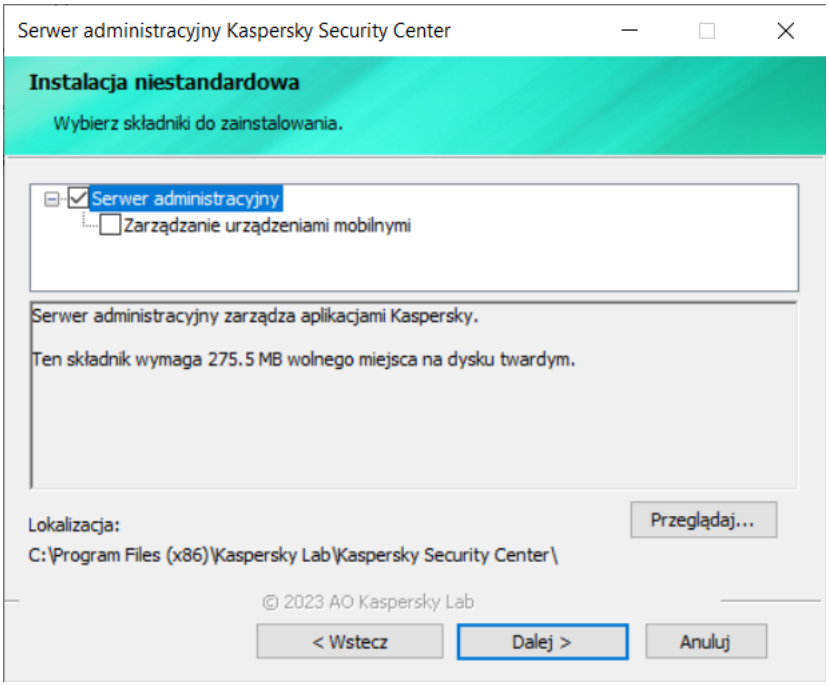
   Jeśli używasz SQL Server jako DBMS dla Serwera administracyjnego, możesz migrować dane z SQL Server do MySQL lub MariaDB DBMS. Aby to zrobić, uruchom narzędzie klbackup w trybie interaktywnym, aby utworzyć kopię zapasową danych. Włącz opcję **Migracja do formatu MySQL/MariaDB** w oknie **Ustawienia kopii zapasowej** kopii zapasowej Kreatora kopii zapasowych i przywracania. Kaspersky Security Center utworzy kopię zapasową kompatybilną z MySQL i MariaDB. Następnie możesz przywrócić dane z kopii zapasowej do MySQL lub MariaDB.

   Możesz również włączyć opcję **Wykonaj migrację do formatu Azure** jeśli chcesz migrować dane z SQL Server do Azure SQL DBMS.
2. Wybierz nowe urządzenie, na którym chcesz zainstalować Serwer administracyjny. Upewnij się, że sprzęt i oprogramowanie na wybranym urządzeniu spełniają wymagania Serwera administracyjnego, Kaspersky Security Center Web Console oraz Agenta sieciowego. Sprawdź również, czy dostępne są porty używane na Serwerze administracyjnym.
3. Na nowym urządzeniu zainstaluj system zarządzania bazą danych (DBMS), z którego będzie korzystał Serwer administracyjny.

   Kiedy wybierasz DBMS, weź pod uwagę liczbę urządzeń obsługiwanych przez Serwer administracyjny.

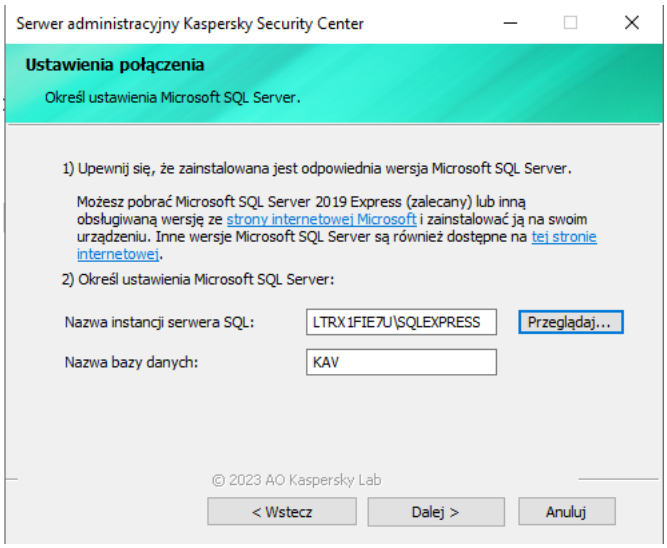
4. Uruchom niestandardową instalację Serwera administracyjnego na nowym urządzeniu.

5. Zainstaluj składniki Serwera administracyjnego w tym samym folderze, w którym Serwer administracyjny jest zainstalowany na poprzednim urządzeniu. Kliknij przycisk **Przeglądaj**, aby określić ścieżkę do pliku.



Okno instalacji niestandardowej

6. Skonfiguruj ustawienia połączenia z serwerem bazy danych.



Przykład okna Ustawienia połączenia dla Microsoft SQL Server

W zależności od tego, gdzie chcesz zlokalizować serwer bazy danych, wykonaj jedną z następujących czynności:

- Przenieś Serwer administracyjny na nowe urządzenie

1. Kliknij przycisk **Przeglądaj** obok pola **Nazwa instancji serwera SQL**, a następnie wybierz nową nazwę urządzenia z wyświetlonej listy.
2. Wprowadź nową nazwę bazy danych w polu **Nazwa bazy danych**.

   Należy pamiętać, że nazwa nowej bazy danych musi być zgodna z nazwą bazy danych z poprzedniego urządzenia. Nazwy baz danych muszą być identyczne, abyś mógł korzystać z kopii zapasowej Serwera administracyjnego. Domyślna nazwa bazy danych to *KAV*.

- Zachowaj serwer bazy danych na poprzednim urządzeniu

  1. Kliknij przycisk **Przeglądaj** obok pola **Nazwa instancji serwera SQL**, a następnie wybierz poprzednią nazwę urządzenia z wyświetlonej listy.

     Pamiętaj, że poprzednie urządzenie musi być dostępne do połączenia z nowym Serwerem administracyjnym.
  2. Wprowadź poprzednią nazwę bazy danych w polu **Nazwa bazy danych**.

7. Po zakończeniu instalacji odzyskaj dane Serwera administracyjnego na nowym urządzeniu za pomocą narzędzia klbackup.

   Jeśli używasz programu SQL Server jako DBMS na poprzednich i nowych urządzeniach, pamiętaj, że wersja programu SQL Server zainstalowana na nowym urządzeniu musi być taka sama lub nowsza niż wersja programu SQL Server zainstalowana na poprzednim urządzeniu. W przeciwnym razie nie będzie możliwe odzyskanie danych Serwera administracyjnego na nowym urządzeniu.
8. Otwórz Kaspersky Security Center Web Console i połącz się z Serwerem administracyjnym.
9. Sprawdź, czy wszystkie urządzenia klienckie są połączone z Serwerem administracyjnym.
10. Odinstaluj Serwer administracyjny i serwer bazy danych z poprzedniego urządzenia.

Możesz także użyć Konsoli administracyjnej do przeniesienia Serwera administracyjnego i serwera bazy danych na inne urządzenie.

Początkowa konfiguracja Kaspersky Security Center Web Console

Ta sekcja opisuje kroki, jakie należy podjąć po zainstalowaniu Kaspersky Security Center Web Console, aby przeprowadzić wstępną konfigurację.

Kreator wstępnej konfiguracji (Kaspersky Security Center Web Console)

Ta sekcja zawiera informacje o działaniu kreatora wstępnej konfiguracji Serwera administracyjnego.

kreator wymaga dostępu do Internetu. Jeżeli Twój Serwer administracyjny nie ma dostępu do Internetu, zalecamy ręczne wykonanie wszystkich kroków kreatora poprzez interfejs konsoli Kaspersky Security Center Web Console.

Kaspersky Security Center umożliwia dostosowanie minimalnego zestawu ustawień niezbędnych do stworzenia systemu scentralizowanego zarządzania ochroną sieci przed zagrożeniami bezpieczeństwa. Taka konfiguracja jest przeprowadzana przez Kreator wstępnej konfiguracji. Przy pierwszym uruchomieniu kreatora możesz wprowadzić w aplikacji następujące zmiany:

- Dodaj pliki klucza lub wprowadź kody aktywacyjne, które mogą być automatycznie przesyłane do urządzeń w grupach administracyjnych.
- Skonfigurować interakcję z Kaspersky Security Network (KSN). Jeśli zezwolono na używanie KSN, kreator uruchomi usługę serwera proxy KSN, która zapewnia połączenie pomiędzy KSN a urządzeniami.
- Skonfigurować dostarczanie powiadomień informujących o zdarzeniach występujących podczas działania Serwera administracyjnego i zarządzanych aplikacji (w celu zapewnienia poprawnego działania opcji dostarczania powiadomień, na Serwerze administracyjnym i wszystkich urządzeniach, na które mają być wysyłane powiadomienia, powinna być włączona usługa Posłaniec).
- Utworzyć zasadę ochrony dla stacji roboczych i serwerów, a także zadania skanowania w poszukiwaniu złośliwego oprogramowania, zadania pobierania uaktualnień i zadania tworzenia kopii zapasowej danych dla najwyższego poziomu hierarchii zarządzanych urządzeń.

  Kreator wstępnej konfiguracji tworzy zasady tylko dla tych aplikacji, dla których folder **Zarządzane urządzenia** nie zawiera żadnych zasad. Kreator wstępnej konfiguracji nie tworzy zadań, jeśli zadania o tych samych nazwach zostały już utworzone dla najwyższego poziomu hierarchii zarządzanych urządzeń.

Po zainstalowaniu Serwera administracyjnego, przy pierwszym nawiązaniu połączenia z nim, aplikacja automatycznie wyświetli pytanie dotyczące uruchomienia kreatora wstępnej konfiguracji. Kreator wstępnej konfiguracji można również uruchomić ręcznie w dowolnym momencie.

W celu ręcznego uruchomienia kreatora wstępnej konfiguracji:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogólne**.

3. Kliknij **Uruchom kreatora wstępnej konfiguracji**.

kreator wyświetli pytanie o przeprowadzenie wstępnej konfiguracji Serwera administracyjnego. Postępuj zgodnie z instrukcjami kreatora. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

Krok 1. Określenie ustawień połączenia internetowego

Określ ustawienia dostępu do Internetu dla Serwera administracyjnego. Należy skonfigurować dostęp do Internetu w taki sposób, aby korzystać z Kaspersky Security Network i pobierać aktualizacje antywirusowych baz danych dla Kaspersky Security Center i zarządzanych aplikacji Kaspersky.

Włącz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest włączona, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

- Adres

  Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

- Numer portu

  Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

- Pomiń serwer proxy dla adresów lokalnych

  Żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

- Uwierzytelnianie na serwerze proxy

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  To pole wejściowe jest dostępne, jeśli opcja **Użyj serwera proxy** jest zaznaczona.

- Nazwa użytkownika

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

- Hasło

  Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

  Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

Możesz skonfigurować dostęp do Internetu później, niezależnie od kreatora wstępnej konfiguracji.

Krok 2. Pobieranie żądanych uaktualnień

Wymagane aktualizacje są automatycznie pobierane z serwerów Kaspersky.

Krok 3. Wybór elementów do zabezpieczenia

Wybierz obszary ochrony i systemy operacyjne używane w Twojej sieci. Jeśli wybierzesz te opcje, określ filtry dla wtyczek zarządzających aplikacjami i pakietami dystrybucyjnymi na serwerach Kaspersky, które możesz pobrać do zainstalowania na urządzeniach klienckich w Twojej sieci. Wybierz opcje:

- Obszary

Możesz wybrać następujące obszary ochrony:

- **Stacje robocze**. Wybierz tę opcję, jeśli chcesz chronić stacje robocze w swojej sieci. Domyślnie zaznaczona jest opcja Stacja robocza.
- **Serwery plików i magazyny**. Wybierz tę opcję, jeśli chcesz chronić serwery plików w swojej sieci.
- **Urządzenia mobilne**. Wybierz tę opcję, jeśli chcesz chronić urządzenia mobilne należące do firmy lub pracowników firmy. Jeśli wybierzesz tę opcję, ale nie dostarczyłeś licencji z funkcją Zarządzanie urządzeniami mobilnymi, zostanie wyświetlona wiadomość informująca o konieczności dostarczenia licencji z funkcją Zarządzanie urządzeniami mobilnymi. Jeśli nie dostarczysz licencji, nie możesz korzystać z funkcji Urządzenia mobilne.
- **Wirtualizacja**. Wybierz tę opcję, jeśli chcesz chronić maszyny wirtualne w swojej sieci.
- **Kaspersky Anti-Spam**. Wybierz tę opcję, jeśli chcesz chronić serwery pocztowe w swojej organizacji przed spamem, szkodliwymi programami i oszukańczymi wiadomościami.
- **Systemy wbudowane**. Wybierz tę opcję, jeśli chcesz chronić wbudowane systemy Windows, takie jak bankomat.
- **Sieci przemysłowe**. Wybierz tę opcję, jeśli chcesz monitorować dane bezpieczeństwa w sieci przemysłowej oraz z punktów końcowych sieci, które są chronione przez aplikacje firmy Kaspersky.
- **Przemysłowe punkty końcowe**. Wybierz tę opcję, jeśli chcesz chronić pojedyncze węzły w sieci przemysłowej.

- Systemy operacyjne

Możesz wybrać następujące platformy:

- Microsoft Windows
- Linux
- macOS
- Android
- Inne

Aby uzyskać informacje na temat obsługiwanych systemów operacyjnych, zobacz Wymagania sprzętowe i programowe dla Kaspersky Security Center Web Console.

Możesz wybrać pakiety aplikacji Kaspersky z listy dostępnych pakietów później, niezależnie od kreatora wstępnej konfiguracji. Aby uprościć wyszukiwanie potrzebnych pakietów, możesz filtrować listę dostępnych pakietów według różnych kryteriów.

Krok 4. Wybieranie szyfrowania w rozwiązaniach

Okno **Szyfrowanie w rozwiązaniach** jest wyświetlane tylko wtedy, gdy wybrano **Stacje robocze** jako obszar ochrony.

Kaspersky Endpoint Security for Windows zawiera narzędzia do szyfrowania informacji przechowywanych na urządzeniach klienckich z systemem Windows. Te narzędzia szyfrujące mają zaimplementowany standard Advanced Encryption Standard (AES) z kluczem o długości 256-bitowej lub 56-bitowej.

Pobieranie i korzystanie z pakietu dystrybucyjnego z kluczem o długości 256 bitów musi odbywać się zgodnie z obowiązującymi przepisami i regulacjami. Aby pobrać pakiet dystrybucyjny Kaspersky Endpoint Security for Windows potrzebny w Twojej organizacji, miej na uwadze ustawodawstwo kraju, w którym znajdują się urządzenia klienckie Twojej organizacji.

W oknie **Szyfrowanie w rozwiązaniach** wybierz jeden z następujących typów szyfrowania:

- Lite encryption (Szyfrowanie podstawowe). Ten typ szyfrowania używa klucza o długości 56 bitów.
- Strong encryption (Silne szyfrowanie). Ten typ szyfrowania używa klucza o długości 256 bitów.

Możesz wybrać pakiet dystrybucyjny dla Kaspersky Endpoint Security for Windows z wymaganym typem szyfrowania później, niezależnie od kreatora wstępnej konfiguracji.

Krok 5. Konfigurowanie instalacji wtyczek dla zarządzanych aplikacji

Wybierz wtyczki dla zarządzanych aplikacji, które mają zostać zainstalowane. Zostanie wyświetlona lista wtyczek znajdujących się na serwerach Kaspersky. Lista jest filtrowana zgodnie z opcjami wybranymi w poprzednim kroku kreatora. Domyślnie, pełna lista zawiera wtyczki we wszystkich językach. Aby wyświetlić tylko wtyczkę w określonym języku, użyj filtru. Lista wtyczek zawiera następujące kolumny:

- **Nazwa**

  Zostały wybrane wtyczki zależne od obszarów ochrony i platform, które wybrano w poprzednim kroku.

- **Wersja**

  Lista zawiera wtyczki we wszystkich wersjach umieszczone na serwerach Kaspersky. Domyślnie zostaną wybrane wtyczki w najnowszych wersjach.

- **Język**

  Domyślnie wersja językowa wtyczki jest definiowana przez wersję językową Kaspersky Security Center, którą wybrałeś w momencie instalacji. Możesz określić inne wersje językowe na liście rozwijalnej **Wskaż język dla Konsoli administracyjnej lub**.

Po wybraniu wtyczek kliknij przycisk **Dalej**, aby rozpocząć instalację.

Wtyczki administracyjne dla aplikacji Kaspersky można zainstalować ręcznie, niezależnie od kreatora wstępnej konfiguracji.

Krok 6. Instalowanie wybranych wtyczek

Kreator wstępnej konfiguracji automatycznie instaluje wtyczki wybrane w poprzednim kroku. Aby zainstalować niektóre wtyczki, należy zaakceptować warunki Umowy licencyjnej. Zapoznaj się z treścią wyświetlonej Umowy licencyjnej, zaznacz pole **Zgadzam się na korzystanie z Kaspersky Security Network** i kliknij przycisk **Zainstaluj**. Jeśli nie akceptujesz warunków Umowy licencyjnej, wtyczka nie zostanie zainstalowana.

Po zainstalowaniu wszystkich wybranych wtyczek Kreator wstępnej konfiguracji automatycznie przeniesie Cię do następnego kroku.

Krok 7. Pobieranie pakietów dystrybucyjnych i tworzenie pakietów instalacyjnych

Wybierz pakiety dystrybucyjne do pobrania.

Dystrybutory zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center.

Po wybraniu typu szyfrowania dla Kaspersky Endpoint Security for Windows, zostanie wyświetlona lista pakietów dystrybucyjnych obu typów szyfrowania. Pakiet dystrybucyjny z wybranym typem szyfrowania zostanie wybrany z listy. Możesz wybrać pakiety dystrybucyjne dowolnego typu szyfrowania. Język pakietu dystrybucyjnego odpowiada językowi Kaspersky Security Center. Jeśli wersja językowa pakietu dystrybucyjnego Kaspersky Endpoint Security for Windows dla Kaspersky Security Center nie istnieje, zostanie wybrana angielska wersja językowa pakietu dystrybucyjnego.

Aby zakończyć pobieranie niektórych pakietów dystrybucyjnych, należy zaakceptować Umowę licencyjną. Jeśli klikniesz przycisk **Zaakceptuj**, zostanie wyświetlona treść Umowy licencyjnej. Aby przejść do kolejnego kroku kreatora, należy zaakceptować warunki i postanowienia Umowy licencyjnej oraz warunki i postanowienia Polityki prywatności Kaspersky. Jeśli nie akceptujesz warunków i postanowień, pobieranie pakietu zostanie anulowane.

Po zaakceptowaniu warunków i postanowień Umowy licencyjnej oraz warunków i postanowień Polityki prywatności Kaspersky, pobieranie pakietów dystrybucyjnych będzie kontynuowane. W późniejszym czasie możesz wykorzystać pakiety instalacyjne do wdrożenia aplikacji Kaspersky na urządzeniach klienckich.

Możesz pobrać pakiety dystrybucyjne i utworzyć pakiety instalacyjne później, niezależnie od kreatora wstępnej konfiguracji.

Krok 8. Konfigurowanie Kaspersky Security Network

Określ ustawienia przekazywania informacji o działaniach Kaspersky Security Center do bazy wiedzy Kaspersky Security Network. Wybierz jedną z następujących opcji:

- **Zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje zainstalowane na urządzeniach klienckich automatycznie prześlą szczegóły swoich działań do Kaspersky Security Network. Uczestnictwo w Kaspersky Security Network umożliwia szybsze aktualizowanie baz danych zawierających informacje o wirusach i innych zagrożeniach, co zapewnia szybszą reakcję na pojawiające się zagrożenia bezpieczeństwa.

- **Nie zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje nie dostarczą informacji do Kaspersky Security Network.

  Jeśli wybierzesz tę opcję, korzystanie z Kaspersky Security Network zostanie wyłączone.

Możesz skonfigurować dostęp do Kaspersky Security Network (KSN) później, niezależnie od kreatora wstępnej konfiguracji.

Krok 9. Wybieranie metody aktywacji aplikacji

Wybierz jedną z poniższych opcji aktywacji Kaspersky Security Center:

- **Wprowadzając kod aktywacyjny**

  Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Możesz wprowadzić kod aktywacyjny w celu dodania klucza aktywującego Kaspersky Security Center. Możesz otrzymać kod aktywacyjny na adres e-mail, który określiłeś po zakupieniu Kaspersky Security Center.

  Aby aktywować aplikację kodem aktywacyjnym, potrzebny jest dostęp do internetu w celu nawiązania połączenia z serwerami aktywacji Kaspersky.

  Jeśli wybrałeś tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w węźle **Licencje Kaspersky** drzewa Konsoli administracyjnej.

- **Określając plik klucza**

  Plik klucza to plik z rozszerzeniem .key, dostarczony przez firmę Kaspersky. Plik klucza jest przeznaczony do dodania klucza aktywującego aplikację.

  Możesz otrzymać plik klucza na adres e-mail, który określiłeś po zakupieniu Kaspersky Security Center.

  Aby aktywować aplikację przy pomocy pliku klucza, nie musisz łączyć się z serwerami aktywacji Kaspersky.

  Jeśli wybrałeś tę opcję aktywacji, możesz włączyć opcję **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.

  Jeśli ta opcja jest włączona, klucz licencyjny zostanie automatycznie zainstalowany na zarządzanych urządzeniach.

  Jeśli ta opcja jest wyłączona, możesz wdrożyć klucz licencyjny na zarządzanych urządzeniach później, w węźle **Licencje Kaspersky** drzewa Konsoli administracyjnej.

- **Odraczając aktywację aplikacji**

  Aplikacja będzie działała z podstawową funkcjonalnością, bez Zarządzania urządzeniami mobilnymi oraz bez Zarządzania systemami.

Jeśli wybierzesz opcję odroczenia aktywacji aplikacji, będziesz mógł dodać klucz licencyjny w późniejszym czasie, wybierając **Operacje** → **Licencjonowanie**.

Podczas pracy z Kaspersky Security Center wdrożonym z płatnego obrazu AMI lub dla Usage-based monthly billed SKU nie można określić pliku klucza ani wprowadzić kodu.

Krok 10. Określanie ustawień zarządzania aktualizacjami firm trzecich

Ten krok nie jest wyświetlany, jeśli nie posiadasz licencji Zarządzanie lukami i poprawkami, a zadanie *Wyszukiwanie luk i wymaganych aktualizacji* już istnieje.

Dla aktualizacji oprogramowania innych firm wybierz jedną z następujących opcji:

- **Wyszukaj wymagane aktualizacje**

  Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie utworzone.

  Opcja ta jest wybrana domyślnie.

- **Wyszukaj i zainstaluj wymagane aktualizacje**

  Zadania *Wyszukiwanie luk i wymaganych aktualizacji* i *Zainstaluj wymagane aktualizacje i napraw luki* są tworzone automatycznie, jeśli ich nie ma.

  Ta opcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

Dla aktualizacji Windows Update wybierz jedną z następujących opcji:

- **Użyj źródeł aktualizacji zdefiniowanych w zasadzie domeny**

  Urządzenia klienckie pobiorą aktualizacje Windows Update zgodnie z ustawieniami zasad domeny. Zasada Agenta sieciowego jest tworzona automatycznie, jeśli jeszcze jej nie masz.

- **Użyj Serwera administracyjnego jako serwera WSUS**

  Urządzenia klienckie pobiorą aktualizacje Windows Update z Serwera administracyjnego. Zadanie *Wykonaj synchronizację Windows Update* i zasada Agenta sieciowego są tworzone automatycznie, jeśli jeszcze ich nie masz.

  Ta opcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

Zadania *Wyszukiwanie luk i wymaganych aktualizacji* oraz *Zainstaluj wymagane aktualizacje i napraw luki* możesz utworzyć niezależnie od kreatora wstępnej konfiguracji. Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie *Wykonaj synchronizację Windows Update* i wybierz opcję **Użyj Serwera administracyjnego jako serwera WSUS** w zasadzie Agenta sieciowego.

Krok 11. Tworzenie podstawowej konfiguracji ochrony sieci

Możesz sprawdzić listę utworzonych zasad i zadań.

Przed przystąpieniem do następnego kroku kreatora poczekaj na zakończenie tworzenia zasad i zadań.

Możesz utworzyć wymagane zadania i zasady później, niezależnie od kreatora wstępnej konfiguracji.

Krok 12. Konfigurowanie powiadomień e-mail

Skonfiguruj dostarczanie powiadomień o zdarzeniach zarejestrowanych podczas działania aplikacji firmy Kaspersky na urządzeniach klienckich. Ustawienia te będą używane jako ustawienia domyślne dla profili aplikacji.

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w aplikacjach firmy Kaspersky użyj następujących ustawień:

- **Adresaci (adresy e-mail)**

  Adresy e-mail użytkowników, którym aplikacja będzie wysyłała powiadomienia. Możesz wprowadzić jeden lub więcej adresów; jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami.

- **Adres serwera SMTP**

  Adres lub adresy serwerów pocztowych Twojej organizacji.

  Jeśli wprowadzisz więcej niż jeden adres, oddziel je średnikami. Możesz użyć następujących wartości:

  - Adres IPv4 lub IPv6
  - Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
  - Nazwa DNS serwera SMTP

- **Port serwera SMTP**

  Numer portu komunikacji serwera SMTP. Jeśli korzystasz z kilku serwerów SMTP, połączenie z nimi jest nawiązywane przez określony port komunikacyjny. Domyślny numer portu to 25.

- **Użyj uwierzytelniania ESMTP**

  Włącza obsługę autoryzacji ESMTP. Po zaznaczeniu opcji, w polach **Nazwa użytkownika** i **Hasło** możesz określić ustawienia autoryzacji ESMTP. Domyślnie pole to nie jest zaznaczone.

- **Użyj TLS**

Możesz określić ustawienia TLS połączenia z serwerem SMTP:

- **Nie używaj TLS**

  Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.

- **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

  Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

- **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**

  Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

  > Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

  Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić certyfikat dla połączenia TLS, klikając odnośnik **Określ certyfikaty**:

- Odszukaj plik certyfikatu serwera SMTP:

  Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

- Odszukaj plik certyfikatu klienta:

  Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

  - Certyfikat X-509:

    Musisz określić plik z certyfikatem oraz plik z kluczem prywatnym. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po załadowaniu obu plików należy określić hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

  - Kontener pkcs12:

    Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

Możesz przetestować nowe ustawienia powiadomień e-mail, klikając przycisk **Wyślij wiadomość testową**.

Możesz skonfigurować powiadomienia o zdarzeniach później, niezależnie od kreatora wstępnej konfiguracji.

Krok 13. Przeprowadzanie przeszukiwania sieci

Serwer administracyjny przeprowadzi wstępne przeszukiwanie. Podczas przeszukiwania wyświetlany jest pasek postępu. Po zakończeniu przeszukiwania, odnośnik **Wyświetl wykryte urządzenia** stanie się dostępny. Możesz kliknąć ten odnośnik, aby przejrzeć urządzenia w sieci wykryte przez Serwer administracyjny. Aby wrócić do kreatora wstępnej konfiguracji, wciśnij klawisz **Escape**.

Możesz wykonać przeszukiwanie sieci później, niezależnie od kreatora wstępnej konfiguracji. Użyj Kaspersky Security Center Web Console, aby skonfigurować przeszukiwanie domen Windows, Active Directory, zakresów IP i sieci IPv6.

Krok 14. Zamykanie kreatora wstępnej konfiguracji

W oknie zakończenia pracy Kreatora wstępnej konfiguracji zaznacz pole **Uruchom kreatora wdrażania ochrony**, jeśli chcesz uruchomić automatyczną instalację aplikacji antywirusowych lub Agenta sieciowego na urządzeniach w sieci.

Aby zamknąć kreator, kliknij przycisk **Zakończ**.

Podłączanie urządzeń mobilnych

Ta sekcja opisuje sposób podłączania zarządzanych urządzeń mobilnych (czyli zarządzanych urządzeń znajdujących się poza siecią główną) z Serwerem administracyjnym.

Scenariusz: Podłączanie urządzeń mobilnych przez bramę połączenia

W tym scenariuszu opisano sposób podłączania zarządzanych urządzeń znajdujących się poza siecią główną z Serwerem administracyjnym.

Wymagania wstępne

Scenariusz ma następujące wymagania wstępne:

- Strefa zdemilitaryzowana (DMZ) jest zorganizowana w sieci Twojej organizacji.
- Serwer administracyjny Kaspersky Security Center jest zainstalowany w sieci firmowej.

Etapy

Ten scenariusz przebiega etapami:

1. **Wybieranie urządzenia kliencka w DMZ**

   To urządzenie zostanie użyte jako brama połączenia. Urządzenie, które wybrałeś, musi spełniać wymagania dla bram połączenia.

2 Instalowanie Agenta sieciowego w roli bramy połączenia

Do zainstalowania Agenta sieciowego na wybranym urządzeniu zalecane jest używanie instalacji lokalnej.

Domyślnie plik instalacyjny znajduje się w następującym miejscu: \\<nazwa serwera>\KLSHARE\PkgInst\NetAgent_<numer wersji>

W oknie **Brama połączenia** kreatora instalacji Agenta sieciowego wybierz **Użyj Agenta sieciowego jako bramy połączenia w DMZ**. Ten tryb jednocześnie aktywuje rolę bramy połączenia i nakazuje Agentowi sieciowemu czekać na połączenia z Serwera administracyjnego zamiast nawiązywać połączenia z Serwerem administracyjnym.

Alternatywnie możesz zainstalować Agenta sieciowego na urządzeniu z systemem Linux i skonfigurować Agenta sieciowego do pracy jako brama połączenia, ale zwróć uwagę na listę ograniczeń Agenta sieciowego działającego na urządzeniach z systemem Linux.

3 Zezwalanie na połączenia w zaporach sieciowych w bramie połączenia

Aby upewnić się, że Serwer administracyjny może faktycznie połączyć się z bramą połączenia w strefie DMZ, zezwolić na połączenia z portem TCP o numerze 13000 we wszystkich zaporach ogniowych między Serwerem administracyjnym a bramą połączenia.

Jeśli brama połączenia nie ma rzeczywistego adresu IP w Internecie, ale zamiast tego znajduje się poza NAT (Network Address Translation — translacja adresów sieciowych), skonfiguruj regułę, aby przekazywać połączenia przez NAT.

4 Tworzenie grupy administracyjnej dla urządzeń zewnętrznych

Utwórz nową grupę w grupie **Zarządzane urządzenia**. Ta nowa grupa będzie zawierała zewnętrzne zarządzane urządzenia.

5 Podłączanie bramy połączenia do Serwera administracyjnego

Brama połączenia, którą skonfigurowałeś, oczekuje na połączenie z Serwera administracyjnego. Jednakże Serwer administracyjny nie wyświetla urządzenia z bramą połączenia wśród zarządzanych urządzeń. Dzieje się tak ponieważ brama połączenia nie próbowała nawiązać połączenia z Serwerem administracyjnym. Dlatego też należy przeprowadzić specjalną procedurę w celu zapewnienia, że Serwer administracyjny zainicjuje połączenie z bramą połączenia.

Wykonaj następujące czynności:

1. Dodaj bramę połączenia jako punkt dystrybucji.
2. Przenieś bramę połączenia z grupy **Urządzenia nieprzypisane** do grupy utworzonej dla urządzeń zewnętrznych.

Brama połączenia została podłączona i skonfigurowana.

6 Podłączanie zewnętrznych komputerów stacjonarnych do Serwera administracyjnego

Zwykle zewnętrzne komputery stacjonarne nie są przenoszone wewnątrz obwodu. Dlatego musisz skonfigurować je tak, aby łączyły się z Serwerem administracyjnym przez bramę podczas instalowania Agenta sieciowego.

7 Konfigurowanie aktualizacji dla zewnętrznych komputerów stacjonarnych

Jeśli aktualizacje aplikacji zabezpieczających są skonfigurowane do pobierania z Serwera administracyjnego, komputery zewnętrzne pobierają aktualizacje przez bramę połączenia. Ma to dwie wady:

- To niepotrzebny ruch, który zajmuje przepustowość kanału komunikacji internetowej firmy.
- Niekoniecznie jest to najszybszy sposób uzyskiwania aktualizacji. Jest bardzo prawdopodobne, że pobieranie aktualizacji z serwerów aktualizacji Kaspersky byłoby tańsze i szybsze.

Wykonaj następujące czynności:

1. Przenieś wszystkie komputery zewnętrzne do oddzielnej grupy administracyjnej, którą utworzyłeś wcześniej.
2. Wyklucz grupę z urządzeniami zewnętrznymi z zadania aktualizacji.
3. Utwórz osobne zadanie aktualizacji dla grupy z urządzeniami zewnętrznymi.

8 **Podłączanie przenośnych laptopów do Serwera administracyjnego**

Przenośne laptopy są czasami w sieci, a czasami poza nią. W celu efektywnego zarządzania należy połączyć je z Serwerem administracyjnym w różny sposób w zależności od ich lokalizacji. Aby efektywnie wykorzystywać ruch sieciowy, muszą również pobierać uaktualnienia z różnych źródeł w zależności od ich lokalizacji.

Należy skonfigurować reguły dla użytkowników mobilnych: profile połączeń i opisy lokalizacji sieciowych. Każda reguła definiuje instancję Serwera administracyjnego, z którym muszą łączyć się przenośne laptopy w zależności od ich lokalizacji oraz instancji Serwera administracyjnego, z którego muszą pobierać aktualizacje.

Informacje o podłączaniu urządzeń mobilnych

Niektóre zarządzane urządzenia zawsze znajdują się poza główną siecią (na przykład, komputery w oddziałach regionalnych firmy; kioski, bankomaty i terminale zainstalowane w różnych punktach sprzedaży; komputery w domowych biurach pracowników). Niektóre urządzenia od czasu do czasu wyjeżdżają poza granicę (na przykład, laptopy użytkowników, którzy odwiedzają oddziały regionalne lub biuro klienta).

Nadal musisz monitorować i zarządzać ochroną urządzeń znajdujących się poza biurem - otrzymywać aktualne informacje o ich stanie ochrony i zapewniać aktualność aplikacji zabezpieczających. Jest to konieczne, ponieważ, na przykład, jeśli do takiego urządzenia ktoś się włamał, gdy znajdowało się poza siecią główną, może stać się platformą do rozprzestrzeniania zagrożeń, gdy tylko połączy się z siecią główną. W celu podłączenia urządzeń mobilnych do Serwera administracyjnego, możesz użyć dwóch metod:

- Brama połączenia w strefie zdemilitaryzowanej (DMZ)

  Zobacz schemat transmisji danych: Serwer administracyjny w sieci LAN, zarządzane urządzenia w internecie, używana brama połączenia

- Serwer administracyjny w strefie DMZ

  Zobacz schemat transmisji danych: Serwer administracyjny w strefie DMZ, zarządzane urządzenia w internecie

Brama połączenia w strefie DMZ

Zalecaną metodą podłączania urządzeń mobilnych do Serwera administracyjnego jest zorganizowanie strefy DMZ w sieci organizacji i zainstalowanie bramy połączenia w strefie DMZ. Urządzenia zewnętrzne nawiążą połączenie z bramą połączenia, a Serwer administracyjny znajdujący się w sieci zainicjuje połączenie z urządzeniami za pośrednictwem bramy połączenia.

W porównaniu z drugą metodą ta jest bezpieczniejsza:

- Nie musisz otwierać dostępu do Serwera administracyjnego spoza sieci.
- Uszkodzona brama połączenia nie stwarza dużego zagrożenia dla bezpieczeństwa urządzeń sieciowych. Brama połączeń w rzeczywistości sama niczym nie zarządza i nie ustanawia żadnych połączeń.

Ponadto brama połączeń nie wymaga wielu zasobów sprzętowych.

Jednakże ta metoda ma bardziej skomplikowany proces konfiguracji:

- Aby urządzenie służyło jako brama połączenia w DMZ, musisz zainstalować Agenta sieciowego i podłączyć go do Serwera administracyjnego w określony sposób.
- Nie będziesz mógł używać tego samego adresu do łączenia się z Serwerem administracyjnym we wszystkich sytuacjach. Poza granicami, będziesz musiał użyć nie tylko innego adresu (adresu bramy połączenia), ale także innego trybu połączenia: przez bramę połączenia.
- Musisz także zdefiniować różne ustawienia połączeń dla laptopów w różnych lokalizacjach.

Serwer administracyjny w strefie DMZ

Inną metodą jest zainstalowanie pojedynczego Serwera administracyjnego w strefie DMZ.

Ta konfiguracja jest mniej bezpieczna niż inna metoda. Aby w tym przypadku zarządzać zewnętrznymi laptopami, Serwer administracyjny musi akceptować połączenia z dowolnego adresu w Internecie. Nadal będzie zarządzać wszystkimi urządzeniami w sieci wewnętrznej, ale z DMZ. Dlatego przejęty Serwer może spowodować ogromne szkody, pomimo niskiego prawdopodobieństwa takiego zdarzenia.

Ryzyko jest znacznie niższe, jeśli Serwer administracyjny w DMZ nie zarządza urządzeniami w sieci wewnętrznej. Taka konfiguracja może być wykorzystana, na przykład, przez usługodawcę do zarządzania urządzeniami klientów.

Możesz chcieć użyć tej metody w następujących przypadkach:

- Jeśli jesteś zaznajomiony z instalacją i konfiguracją Serwera administracyjnego i nie chcesz wykonywać innej procedury instalacji i konfiguracji bramy połączenia.
- Jeśli potrzebujesz zarządzać większą liczbą urządzeń. Maksymalna pojemność Serwera administracyjnego to 100 000 urządzeń, podczas gdy brama połączenia może obsługiwać do 10 000 urządzeń.

To rozwiązanie ma również możliwe trudności:

- Serwer administracyjny wymaga większej ilości zasobów sprzętowych i jeszcze jednej bazy danych.
- Informacje o urządzeniach będą przechowywane w dwóch niepowiązanych bazach danych (dla Serwera administracyjnego w sieci i jednej w DMZ), co komplikuje monitorowanie.
- Aby zarządzać wszystkimi urządzeniami, Serwer administracyjny musi być połączony w hierarchię, co komplikuje nie tylko monitorowanie, ale także zarządzanie. Instancja podrzędnego Serwera administracyjnego nakłada ograniczenia na możliwe struktury grup administracyjnych. Musisz zdecydować, w jaki sposób i które zadania i zasady mają być dystrybuowane do instancji podrzędnego Serwera administracyjnego.
- Skonfigurowanie urządzeń zewnętrznych do używania Serwera administracyjnego w DMZ z zewnątrz oraz do używania głównego Serwera administracyjnego od wewnątrz nie jest prostsze niż zwykłe skonfigurowanie ich tak, aby używały warunkowego połączenia przez bramę.
- Wysokie zagrożenia bezpieczeństwa. Zagrożona instancja Serwera administracyjnego ułatwia włamanie się do zarządzanych laptopów. Jeśli tak się stanie, hakerzy muszą tylko poczekać, aż jeden z laptopów wróci do sieci firmowej, aby mogli kontynuować atak na sieć lokalną.

Podłączanie zewnętrznych komputerów stacjonarnych do Serwera administracyjnego

Komputery stacjonarne, które zawsze znajdują się poza główną siecią (na przykład, komputery w oddziałach regionalnych firmy; kioski, bankomaty i terminale zainstalowane w różnych punktach sprzedaży; komputery w domowych biurach pracowników) nie mogą być podłączane bezpośrednio do Serwera administracyjnego. Muszą być podłączeni do Serwera administracyjnego przez bramę połączenia zainstalowaną w strefie zdemilitaryzowanej (DMZ). Ta konfiguracja jest wykonywana podczas instalacji Agenta sieciowego na tych komputerach.

W celu podłączenia zewnętrznych komputerów stacjonarnych do Serwera administracyjnego:

1. Utwórz nowy pakiet instalacyjny dla Agenta sieciowego.
2. Otwórz właściwości utworzonego pakietu instalacyjnego i przejdź do sekcji **Ustawienia** → **Zaawansowane**, a następnie wybierz opcję **Połącz z Serwerem administracyjnym korzystając z bramy połączenia**.

   Ustawienie **Połącz z Serwerem administracyjnym korzystając z bramy połączenia** jest niekompatybilne z ustawieniem **Użyj Agenta sieciowego jako bramy połączenia w DMZ**. Nie możesz włączyć obu tych ustawień jednocześnie.

3. W sekcji **Adres bramy połączenia** określ publiczny adres bramy połączenia.

   Jeśli brama połączenia znajduje się za translacją adresów sieciowych (NAT) i nie ma własnego adresu publicznego, skonfiguruj regułę bramy NAT w celu przekazywania połączeń z adresu publicznego na adres wewnętrzny bramy połączenia.

4. Utwórz autonomiczny pakiet instalacyjny w oparciu o utworzony pakiet instalacyjny.
5. Dostarcz autonomiczny pakiet instalacyjny na komputery docelowe elektronicznie lub na dysku wymiennym.
6. Zainstaluj Agenta sieciowego z pakietu autonomicznego.

Zewnętrzne komputery stacjonarne są połączone z Serwerem administracyjnym.

Informacje o profilach połączenia dla użytkowników mobilnych

Mobilni użytkownicy laptopów (zwanych dalej również "urządzeniami") mogą potrzebować zmiany metody łączenia się z Serwerem administracyjnym lub przełączania pomiędzy Serwerami administracyjnymi w zależności od aktualnej lokalizacji urządzenia w sieci firmowej.

Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

Używanie różnych adresów jednego Serwera administracyjnego

Urządzenia z zainstalowanym Agentem sieciowym mogą łączyć się z Serwerem administracyjnym z poziomu wewnętrznej sieci organizacji lub Internetu. W tej sytuacji wymagane może być, aby Agent sieciowy używał innych adresów do łączenia się z Serwerem administracyjnym: zewnętrznego adresu Serwera administracyjnego dla połączenia internetowego oraz wewnętrznego adresu Serwera administracyjnego dla wewnętrznego połączenia sieciowego.

W tym celu we właściwościach profilu agenta sieciowego dodaj profil do łączenia się z serwerem administracyjnym (w sekcji **Ustawienia aplikacji → Łączność → Profile połączenia → Profile połączeń Serwera administracyjnego**. W oknie tworzenia profilu wyłącz opcję **Użyj tylko do pobierania aktualizacji** i upewnij się, że opcja **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu** jest wybrana. Jeśli do łączenia się z Serwerem administracyjnym używasz bramy połączenia (na przykład, w konfiguracji Kaspersky Security Center, opisanej w sekcji Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej), w odpowiednim polu profilu połączenia musisz określić adres bramy połączenia.

Przełączanie pomiędzy Serwerami administracyjnymi w zależności od aktualnej sieci

Jeśli organizacja posiada kilka biur z różnymi Serwerami administracyjnymi, a niektóre urządzenia z zainstalowanym Agentem sieciowym są przenoszone pomiędzy nimi, Agent sieciowy musi łączyć się z Serwerem administracyjnym sieci lokalnej w biurze, w którym znajduje się urządzenie.

W tej sytuacji konieczne jest utworzenie profilu dla połączenia z serwerem administracyjnym we właściwościach zasad agenta sieciowego dla każdego z biur, za wyjątkiem głównego biura, w którym znajduje się oryginalny macierzysty serwer administracyjny. W profilach połączenia należy określić adresy serwerów administracyjnych i włączyć lub wyłączyć opcję **Użyj tylko do pobierania aktualizacji**:

- Wybierz tę opcję, jeśli chcesz, aby Agent sieciowy zsynchronizował się z macierzystym Serwerem administracyjnym, a Serwer lokalny był używany tylko do pobierania uaktualnień.
- Wyłącz tę opcję, jeśli Agent sieciowy ma być całkowicie zarządzany przez lokalny Serwer administracyjny.

Następnie powinieneś ustalić warunki przełączania do nowo utworzonych profili: przynajmniej jeden warunek dla każdego z biur, za wyjątkiem głównego biura. Celem każdego warunku jest wykrycie elementów, które są specyficzne dla środowiska sieciowego w biurze. Jeśli warunek jest prawdziwy, odpowiedni profil zostaje aktywowany. Jeśli żaden z warunków nie jest prawdziwy, Agent sieciowy przełączy się do macierzystego Serwera administracyjnego.

Tworzenie profilu połączenia dla użytkowników mobilnych

Profil połączenia serwera administracyjnego jest dostępny tylko na urządzeniach działających pod kontrolą systemu Windows i macOS.

W celu utworzenia profilu połączenia Agenta sieciowego z Serwerem administracyjnym dla użytkowników mobilnych:

1. Jeżeli chcesz utworzyć profil połączenia dla grupy zarządzanych urządzeń, otwórz zasadę agenta sieciowego tej grupy. W tym celu wykonaj następujące czynności:
   a. W menu głównym przejdź do **Urządzenia → Profile zasad**.
   b. Kliknij łącze bieżącej ścieżki.
   c. W oknie, które zostanie otwarte, wybierz żądaną grupę administracyjną.
      Następnie bieżąca ścieżka zostanie zmieniona.
   d. Dodaj zasadę agenta sieciowego dla grupy zarządzanych urządzeń. Jeśli już ją utworzono, kliknij nazwę zasady agenta sieciowego, aby otworzyć właściwości zasady.

2. Jeśli chcesz utworzyć profil połączenia dla konkretnego zarządzanego urządzenia, wykonaj następujące czynności:

   a. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.

   b. Kliknij nazwę zarządzanego urządzenia.

   c. W otwartym oknie właściwości zarządzanego urządzenia kliknij zakładkę **Aplikacje**.

   d. Kliknij nazwę zasady agenta sieciowego, której dotyczy tylko wybrane zarządzane urządzenie.

3. W otwartym oknie właściwości przejdź do **Ustawienia aplikacji** → **Łączność** → **Profile połączenia.**

4. W grupie ustawień **Profile połączeń Serwera administracyjnego** kliknij przycisk **Dodaj**.

   Domyślnie, lista profili połączeń zawiera profile <Tryb offline> i <Macierzysty serwer administracyjny>. Profili nie można modyfikować ani usunąć.

   Profil <Tryb offline> nie określa żadnego Serwera do nawiązania połączenia. Dlatego też, Agent sieciowy, gdy zostaje przełączony do tego profilu, nie próbuje nawiązać połączenia z żadnym Serwerem administracyjnym, gdy aplikacje zainstalowane na urządzeniach klienckich działają pod kontrolą zasad użytkownika mobilnego. Profil <Tryb offline> może być używany, jeśli urządzenia są odłączone od sieci.

   Profil <Macierzysty serwer administracyjny> określa połączenie z serwerem administracyjnym, który został wybrany podczas instalacji agenta sieciowego. Profil <Macierzysty serwer administracyjny> jest stosowany, gdy urządzenie jest ponownie podłączane do macierzystego Serwera administracyjnego po tym, jak przez jakiś czas działało w sieci zewnętrznej.

5. W otwartym oknie **Konfiguruj profil** skonfiguruj profil połączenia:

   - **Konfiguruj profil**

     W tym polu możesz przejrzeć lub zmienić nazwę profilu połączenia.

   - **Adres Serwera administracyjnego**

     Adres Serwera administracyjnego, z którym urządzenie klienckie musi łączyć się podczas aktywacji profilu.

   - **Numer portu**

     Numer portu używanego do nawiązywania połączenia.

   - **Port SSL**

     Numer portu połączenia podczas używania portu SSL.

   - **Użyj połączenia SSL**

     Jeśli ta opcja jest włączona, połączenie jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

     Domyślnie opcja ta jest włączona. Zalecamy, aby nie wyłączać tej opcji, aby Twoje połączenie pozostało bezpieczne.

- Wybierz opcję **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli ta opcja jest wybrana, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

  - Adres

    Adres serwera proxy używanego do łączenia Kaspersky Security Center z Internetem.

  - Numer portu

    Numer portu, poprzez który zostanie nawiązane połączenie proxy Kaspersky Security Center.

  - Uwierzytelnianie na serwerze proxy

    Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  - Nazwa użytkownika

    Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest wybrane).

  - Hasło

    Hasło ustawione przez użytkownika, którego konto jest używane do nawiązywania połączenia z serwerem proxy (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone).

    Aby zobaczyć wprowadzone hasło, trzymaj kliknięty przycisk **Pokaż** tak długo, jak potrzebujesz.

- Adres bramy połączenia

  Adres bramy, poprzez którą urządzenia klienckie łączą się z Serwerem administracyjnym.

- Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny

  Zaznacz to pole, aby zezwolić aplikacjom zainstalowanym na urządzeniu klienckim na korzystanie z profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego, za każdym razem, gdy serwer administracyjny nie jest dostępny. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie pole to nie jest zaznaczone.

- Użyj tylko do pobierania uaktualnień

Jeżeli ta opcja jest włączona, profil będzie używany tylko do pobierania aktualizacji przez aplikacje zainstalowane na urządzeniu klienckim. Dla innych działań połączenie z Serwerem administracyjnym będzie nawiązywane z użyciem wstępnych ustawień określonych podczas instalacji Agenta sieciowego.

Domyślnie opcja ta jest włączona.

- Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu

  Jeśli ta opcja jest włączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu ustawień określonych we właściwościach profilu.

  Jeśli ta opcja jest wyłączona, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym przy użyciu oryginalnych ustawień określonych podczas instalacji.

  Ta opcja jest dostępna, jeśli opcja **Użyj tylko do pobierania uaktualnień** jest wyłączona.

  Domyślnie opcja ta jest wyłączona.

Profil połączenia Agenta sieciowego z Serwerem administracyjnym zostanie utworzony dla użytkowników mobilnych. Jeśli agent sieciowy łączy się z serwerem administracyjnym przy użyciu tego profilu, aplikacje zainstalowane na urządzeniu klienckim będą używać zasad dla urządzeń w trybie użytkownika mobilnego lub zasad użytkownika mobilnego.

Informacje o przełączaniu Agenta sieciowego na inne Serwery administracyjne

Kaspersky Security Center oferuje opcję przełączania Agenta sieciowego na urządzeniu klienckim na inne Serwery administracyjne, jeśli następujące ustawienia sieci zostały zmienione:

- **Warunek dla adresu serwera DHCP** — zmiana adresu IP serwera sieciowego (DHCP).
- **Warunek dla adresu domyślnej bramy połączenia** — zmiana adresu głównej bramy sieci.
- **Warunek dla domeny DNS** — zmiana sufiksu DNS podsieci.
- **Warunek dla adresu serwera DNS** — zmiana adresu IP serwera sieciowego DNS.
- **Warunek dla adresu serwera WINS** — zmiana adresu IP sewera sieciowego WINS. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.
- **Warunek dla rozwiązania nazw** — zmiana nazwy DNS lub NetBIOS urządzenia klienckiego.
- **Warunek dla podsieci** — zmiana adresu i maski podsieci.
- **Warunek dla dostępności domeny Windows** — zmiana stanu domeny systemu Windows, do której podłączone jest urządzenie klienckie. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.
- **Warunek dla dostępności adresu połączenia SSL** — urządzenie klienckie może lub nie może (w zależności od wybranej opcji) nawiązać połączenie SSL z określonym serwerem (nazwa:port). Dla każdego serwera możesz dodatkowo określić certyfikat SSL. W takim przypadku Agent sieciowy weryfikuje certyfikat Serwera, oprócz sprawdzenia możliwości połączenia SSL. Jeśli certyfikat nie pasuje, połączenie nie powiedzie się.

Ta funkcja jest obsługiwana tylko w przypadku agentów sieciowych zainstalowanych na urządzeniach z systemem Windows lub macOS.

Początkowe ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są definiowane podczas instalacji Agenta sieciowego. Następnie, jeśli reguły przełączania Agenta sieciowego na inne Serwery administracyjne zostały zmienione, Agent sieciowy odpowiada na zmiany w ustawieniach sieci w następujący sposób:

- Jeśli ustawienia sieci pokrywają się z ustawieniami jednej z utworzonych reguł, Agent sieciowy nawiąże połączenie z Serwerem administracyjnym określonym w tej regule. Aplikacje zainstalowane na urządzeniach klienckich przełączają się do zasady użytkownika mobilnego pod warunkiem, że takie zachowanie jest dozwolone przez regułę.
- Jeśli nie jest stosowana żadna z reguł, Agent sieciowy przywróci ustawienia domyślne połączenia z Serwerem administracyjnym określone podczas instalacji. Aplikacje zainstalowane na urządzeniach klienckich przywracają aktywne profile.
- Jeśli Serwer administracyjny jest niedostępny, Agent sieciowy używa zasad użytkownika mobilnego.

Agent sieciowy przełącza się do zasady użytkownika mobilnego tylko wtedy, gdy opcja **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny** jest włączona w ustawieniach zasady Agenta sieciowego.

Ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym są zapisywane w profilu połączenia. W profilu połączenia możesz utworzyć reguły przełączania urządzeń klienckich do zasad użytkownika mobilnego, a także skonfigurować profil tak, aby mógł być używany tylko do pobierania uaktualnień.

Tworzenie reguły przełączania Agenta sieciowego według lokalizacji sieciowej

Przełączanie agenta sieciowego według lokalizacji sieciowej jest dostępne tylko na urządzeniach działających pod kontrolą systemu Windows i macOS.

W celu utworzenia reguły przełączania Agenta sieciowego z jednego z Serwera administracyjnego na inny w przypadkui zmiany ustawień sieciowych:

1. Jeśli chcesz utworzyć regułę dla grupy zarządzanych urządzeń, otwórz zasadę agenta sieciowego tej grupy. W tym celu wykonaj następujące czynności:
   a. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
   b. Kliknij łącze bieżącej ścieżki.
   c. W oknie, które zostanie otwarte, wybierz żądaną grupę administracyjną.
      Następnie bieżąca ścieżka zostanie zmieniona.
   d. Dodaj zasadę agenta sieciowego dla grupy zarządzanych urządzeń. Jeśli już ją utworzono, kliknij nazwę zasady agenta sieciowego, aby otworzyć właściwości zasady.
2. Jeśli chcesz utworzyć regułę dla określonego zarządzanego urządzenia, wykonaj następujące czynności:
   a. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.

b. Kliknij nazwę zarządzanego urządzenia.

c. W otwartym oknie właściwości zarządzanego urządzenia kliknij zakładkę **Aplikacje**.

d. Kliknij nazwę zasady agenta sieciowego, której dotyczy tylko wybrane zarządzane urządzenie.

3. W otwartym oknie właściwości przejdź do **Ustawienia aplikacji** → **Łączność** → **Profile połączenia.**

4. W sekcji **Ustawienia lokalizacji sieciowej** kliknij przycisk **Dodaj**.

5. W otwartym oknie właściwości skonfiguruj opis lokalizacji sieciowej i regułę przełączania. Określ następujące ustawienia opisu lokalizacji sieciowej:

   - Opis

     Nazwa opisu lokalizacji sieciowej nie może być dłuższa niż 255 znaków i nie może zawierać znaków specjalnych, takich jak ("*<>?\/:|).

   - Użyj profilu połączenia

     Na liście rozwijalnej możesz określić profil połączenia, którego Agent sieciowy używa do nawiązania połączenia z Serwerem administracyjnym. Ten profil będzie używany, jeśli spełnione są warunki opisu lokalizacji sieciowej. Profil połączenia zawiera ustawienia połączenia Agenta sieciowego z Serwerem administracyjnym i definiuje, kiedy urządzenia klienckie muszą przełączyć się do zasad użytkownika mobilnego. Profil jest używany tylko do pobierania uaktualnień.

   - Opis włączony

     Zaznacz to pole wyboru, aby umożliwić korzystanie z nowego opisu lokalizacji sieciowej.

6. Wybierz warunki reguły przełączania agenta sieciowego:

   - **Warunek dla adresu serwera DHCP** — zmiana adresu IP serwera sieciowego (DHCP).
   - **Warunek dla adresu domyślnej bramy połączenia** — zmiana adresu głównej bramy sieci.
   - **Warunek dla domeny DNS** — zmiana sufiksu DNS podsieci.
   - **Warunek dla adresu serwera DNS** — zmiana adresu IP serwera sieciowego DNS.
   - **Warunek dla adresu serwera WINS** — zmiana adresu IP sewera sieciowego WINS. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.
   - **Warunek dla rozwiązania nazw** — zmiana nazwy DNS lub NetBIOS urządzenia klienckiego.
   - **Warunek dla podsieci** — zmiana adresu i maski podsieci.
   - **Warunek dla dostępności domeny Windows** — zmiana stanu domeny systemu Windows, do której podłączone jest urządzenie klienckie. To ustawienie jest dostępne tylko dla urządzeń z systemem Windows.
   - **Warunek dla dostępności adresu połączenia SSL** — urządzenie klienckie może lub nie może (w zależności od wybranej opcji) nawiązać połączenie SSL z określonym serwerem (nazwa:port). Dla każdego serwera możesz dodatkowo określić certyfikat SSL. W takim przypadku Agent sieciowy weryfikuje certyfikat

Serwera, oprócz sprawdzenia możliwości połączenia SSL. Jeśli certyfikat nie pasuje, połączenie nie powiedzie się.

Warunki w regule są połączone przy użyciu operatora logicznego I. Aby wyzwolić regułę przełączania według opisu lokalizacji sieciowej, muszą być spełnione wszystkie warunki przełączania reguły.

7. W sekcji warunku określ, kiedy agent sieciowy powinien zostać przełączony na inny serwer administracyjny. W tym celu kliknij przycisk **Dodaj**, a następnie ustaw wartość warunku.

   Ponadto opcja **Zgodny z przynajmniej jedną wartością z listy** jest domyślnie włączona. Możesz wyłączyć tę opcję, jeśli chcesz, aby warunek został spełniony ze wszystkimi określonymi wartościami.

8. Zapisz zmiany.

Zostanie utworzona nowa reguła przełączania według opisu lokalizacji sieciowej. Za każdym razem, gdy zostaną spełnione warunki reguły, Agent sieciowy będzie używał profilu połączenia, określonego w regule, do łączenia się z Serwerem administracyjnym.

Kreator wdrażania ochrony

Do zainstalowania aplikacji firmy Kaspersky można użyć kreatora wdrażania ochrony. Kreator wdrażania ochrony umożliwia przeprowadzenie zdalnej instalacji aplikacji przy pomocy specjalnie utworzonych pakietów instalacyjnych lub bezpośrednio z pakietu dystrybucyjnego.

Kreator wdrażania ochrony wykonuje następujące działania:

- Pobiera pakiet instalacyjny potrzebny do zainstalowania aplikacji (jeśli nie został utworzony wcześniej). Pakiet instalacyjny znajduje się w: **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**. Możesz użyć tego pakietu instalacyjnego do przyszłej instalacji aplikacji.

- Tworzy i uruchamia zadanie zdalnej instalacji dla określonych urządzeń lub grupy administracyjnej. Nowo utworzone zadanie zdalnej instalacji jest przechowywane w sekcji **Zadania**. Możesz później uruchomić to zadanie ręcznie. Typ zadania to **Zdalna instalacja aplikacji**.

Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

Uruchamianie kreatora wdrażania ochrony

W celu ręcznego uruchomienia kreatora wdrażania ochrony:

W głównym menu kliknij **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Kreator wdrażania ochrony**.

Zostanie uruchomiony kreatora wdrażania ochrony. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

Krok 1. Wybieranie pakietu instalacyjnego

Wybierz pakiet instalacyjny aplikacji, którą chcesz zainstalować.

Jeśli nie ma pakietu instalacyjnego żądanej aplikacji, kliknij przycisk **Dodaj**, a następnie wybierz aplikację z listy.

Krok 2. Wybieranie metody rozsyłania pliku klucza lub kodu aktywacyjnego

Wybierz metodę rozesłania pliku klucza lub kodu aktywacyjnego:

- **Nie dodawaj klucza licencyjnego do pakietu instalacyjnego**

  Klucz jest automatycznie rozsyłany na wszystkie urządzenia, z którymi jest kompatybilny:
  - Jeśli we właściwościach klucza jest włączona automatyczna dystrybucja.
  - Jeśli utworzono zadanie **Dodaj klucz**.

- **Dodaj klucz licencyjny do pakietu instalacyjnego**

  Klucz jest rozsyłany na urządzenia wraz z pakietem instalacyjnym.

  Nie zalecamy rozpowszechniania klucza przy użyciu tej metody, ponieważ współdzielone prawa dostępu do odczytu są włączone do repozytorium pakietów instalacyjnych.

Jeśli pakiet instalacyjny już zawiera plik klucza lub kod aktywacyjny, to okno zostanie wyświetlone, ale będzie zawierało tylko szczegóły klucza licencyjnego.

Krok 3. Wybieranie wersji Agenta sieciowego

Jeśli wybrałeś pakiet instalacyjny aplikacji innej niż Agent sieciowy, musisz także zainstalować Agenta sieciowego, który łączy aplikację z Serwerem administracyjnym Kaspersky Security Center.

Wybierz najnowszą wersję Agenta sieciowego.

Krok 4. Wybór urządzeń

Określ listę urządzeń, na których zostanie zainstalowana aplikacja:

- **Zainstaluj na zarządzanych urządzeniach**

  Jeżeli ta opcja jest zaznaczona, zadanie zdalnej instalacji jest tworzone dla grupy urządzeń.

- Wybierz urządzenia do instalacji

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

Krok 5. Określanie ustawień zadania zdalnej instalacji

W oknie **Ustawienia zadania zdalnej instalacji** określ ustawienia zdalnej instalacji aplikacji.

W grupie ustawień **Wymuś pobranie pakietu instalacyjnego** określ sposób rozsyłania na urządzenia klienckie plików, które są niezbędne do zainstalowania aplikacji:

- Przy użyciu Agenta sieciowego

  Jeśli ta opcja jest włączona, pakiety instalacyjne są dostarczane na urządzenia klienckie przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

  Jeśli ta opcja jest wyłączona, pakiety instalacyjne są dostarczane przy użyciu narzędzi systemu operacyjnego urządzeń klienckich.

  Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń z zainstalowanymi Agentami sieciowymi.

  Domyślnie opcja ta jest włączona.

- Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji

  Jeśli ta opcja jest włączona, pakiety instalacyjne są przesyłane na urządzenia klienckie przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjnych. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

  Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego są niedostępne.

  Domyślnie ta opcja jest włączona dla zadań zdalnej instalacji utworzonych na wirtualnym Serwerze administracyjnym.

- Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny

  Jeśli ta opcja jest włączona, pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego urządzeń klienckich za pośrednictwem Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci co Serwer administracyjny.

  Domyślnie opcja ta jest włączona.

Określ ustawienia dodatkowe:

- Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana

Jeśli ta opcja jest włączona, wybrana aplikacja nie zostanie ponownie zainstalowana, jeśli już jest zainstalowana na tym urządzeniu klienckim.

Jeśli ta opcja jest wyłączona, aplikacja zostanie zainstalowana mimo wszystko.

Domyślnie opcja ta jest włączona.

- Przypisz pakiet instalacyjny do zasad grupy Active Directory

  Jeśli ta opcja jest włączona, pakiet instalacyjny jest instalowany przy użyciu zasad grupy Active Directory.

  Ta opcja jest dostępna, jeśli wybrany jest pakiet instalacyjny Agenta sieciowego.

  Domyślnie opcja ta jest wyłączona.

Krok 6. Zarządzanie ponownym uruchomieniem

Określ działanie, jakie ma zostać wykonane, jeśli system operacyjny musi być uruchomiony ponownie podczas instalowania aplikacji:

- Nie uruchamiaj ponownie urządzenia

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- Uruchom urządzenie ponownie

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- Pytaj użytkownika o akcję

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - Ponawiaj pytanie co (min)

Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- Uruchom ponownie po (min)

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- Wymuś zamknięcie aplikacji dla zablokowanych sesji

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

Krok 7. Usuwanie niekompatybilnych aplikacji przed instalacją

Ten krok jest dostępny tylko wtedy, gdy wiadomo, że aplikacja, którą instalujesz, jest niekompatybilna z innymi aplikacjami.

Wybierz opcję, jeśli chcesz, aby program Kaspersky Security Center automatycznie usuwał aplikacje, które są niekompatybilne z instalowaną aplikacją.

Lista niekompatybilnych aplikacji także zostanie wyświetlona.

Jeśli nie wybierzesz tej opcji, aplikacja zostanie zainstalowana tylko na urządzeniach, na których nie ma niekompatybilnych aplikacji.

Krok 8. Przenoszenie urządzeń do grupy Zarządzane urządzenia

Określ, czy urządzenia powinny zostać przeniesione do grupy administracyjnej po zainstalowaniu Agenta sieciowego.

- Nie przenoś urządzeń

Urządzenia pozostają w grupach, w których aktualnie się znajdują. Urządzenia, które zostały umieszczone w dowolnej grupie, pozostaną nieprzypisane.

- **Przenieś nieprzypisane urządzenia do grupy**

  Urządzenia są przenoszone do wybranej grupy administracyjnej.

Opcja **Nie przenoś urządzeń** została wybrana domyślnie. W celach bezpieczeństwa możesz ręcznie przenieść urządzenia.

Krok 9. Wybieranie konta w celu uzyskania dostępu do urządzeń

Jeśli to konieczne, dodaj konta, które będą używane do uruchamiania zadania zdalnej instalacji:

- **Konto nie jest wymagane (Agent sieciowy jest zainstalowany)**

  Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

  Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

- **Konto wymagane (Agent sieciowy nie jest używany)**

  Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisano zadanie zdalnej instalacji. W takim przypadku możesz określić konto użytkownika, aby zainstalować aplikację.

  Aby określić konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji, kliknij przycisk **Dodaj**, wybierz **Konto lokalne**, a następnie określ poświadczenia konta użytkownika.

  Możesz określić kilka kont użytkowników, na przykład, jeśli żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, dla których definiujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

Krok 10. Uruchamianie instalacji

Ten krok to ostatni krok kreatora. W tym kroku **Zadanie zdalnej instalacji** zostało pomyślnie utworzone i skonfigurowane.

Domyślnie opcja **Uruchom zadanie po zakończeniu działania kreatora** nie jest zaznaczona. Jeśli wybierzesz tę opcję, **Zadanie zdalnej instalacji** zostanie uruchomione natychmiast po zakończeniu działania kreatora. Jeśli nie wybierzesz tej opcji, **Zadanie zdalnej instalacji** nie zostanie uruchomione. Możesz później uruchomić to zadanie ręcznie.

Kliknij **OK**, aby zakończyć ostatni krok kreatora wdrażania ochrony.

Wdrażanie aplikacji Kaspersky poprzez Kaspersky Security Center Web Console

W tej sekcji opisano sposób wdrażania aplikacji Kaspersky na urządzeniach klienckich w Twojej organizacji przy użyciu Kaspersky Security Center Web Console.

Scenariusz: Wdrażanie aplikacji Kaspersky poprzez Kaspersky Security Center Web Console

Ten scenariusz wyjaśnia sposób wdrażania aplikacji Kaspersky za pośrednictwem Kaspersky Security Center Web Console. Możesz użyć kreatora wstępnej konfiguracji i kreatora wdrażania ochrony lub możesz ręcznie wykonać wszystkie niezbędne kroki.

Do zdalnego zainstalowania przy użyciu Kaspersky Security Center Web Console dostępne są następujące aplikacje:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

Etapy

Wdrożenie aplikacji firmy Kaspersky odbywa się w krokach:

1. **Pobranie wtyczki zarządzającej dla aplikacji**

   Ten krok jest częścią kreatora wstępnej konfiguracji. Jeśli zdecydujesz się nie uruchamiać kreatora, ręcznie pobierz wtyczkę dla Kaspersky Endpoint Security for Windows.

   Jeśli planujesz zarządzać firmowymi urządzeniami mobilnymi, postępuj zgodnie z instrukcjami podanymi w pomocy dla Kaspersky Security for Mobile w celu pobrania i zainstalowania wtyczek zarządzających dla Kaspersky Endpoint Security for Android.

2. **Pobieranie i tworzenie pakietów instalacyjnych**

   Ten krok jest częścią kreatora wstępnej konfiguracji.

   Kreator wstępnej konfiguracji umożliwia pobranie pakietu instalacyjnego z wtyczką zarządzającą. Jeśli nie wybrano tej opcji podczas uruchamiania kreatora lub jeśli w ogóle nie uruchomiono kreatora, musisz ręcznie pobrać pakiet.

   Jeśli nie możesz zainstalować aplikacji firmy Kaspersky przy użyciu Kaspersky Security Center na niektórych urządzeniach, na przykład, na zdalnych urządzeniach pracowników, możesz utworzyć autonomiczne pakiety instalacyjne dla aplikacji. Jeśli używasz autonomicznych pakietów do instalacji aplikacji Kaspersky, nie musisz tworzyć i uruchamiać zadania zdalnej instalacji, ani tworzyć i konfigurować zadań dla Kaspersky Endpoint Security for Windows.

3. **Tworzenie, konfigurowanie i uruchamianie zadania zdalnej instalacji**

   Dla Kaspersky Endpoint Security for Windows ten krok jest częścią kreatora wdrażania ochrony, który jest uruchamiany automatycznie po zakończeniu pracy kreatora wstępnej konfiguracji. Jeśli zdecydujesz się nie uruchamiać Kreator wdrażania ochrony, musisz ręcznie utworzyć to zadanie oraz ręcznie je skonfigurować.

Możesz także ręcznie utworzyć kilka zadań zdalnej instalacji dla różnych grup administracyjnych lub różnych wyborów urządzeń. Możesz wdrożyć różne wersje jednej aplikacji w tych zadaniach.

Upewnij się, że wszystkie urządzenia w Twojej sieci zostały wykryte, a następnie uruchom zadanie zdalnej instalacji (lub zadania).

Jeśli chcesz zainstalować Agenta sieciowego na urządzeniach z systemem operacyjnym SUSE Linux Enterprise Server 15, w pierwszej kolejności zainstaluj pakiet insserv-compat, aby skonfigurować Agenta sieciowego.

4. **Tworzenie i konfigurowanie zadań dla zarządzanej aplikacji**

   Należy skonfigurować zadanie *Zainstaluj aktualizacje programu* Kaspersky Endpoint Security for Windows.

   Ten krok jest częścią kreatora wstępnej konfiguracji: zadanie jest tworzone i konfigurowane automatycznie z domyślnymi ustawieniami. Jeśli nie uruchomiono kreatora, musisz ręcznie utworzyć to zadanie oraz ręcznie je skonfigurować. Jeśli użyjesz kreatora wstępnej konfiguracji, upewnij się, że terminarz zadania spełnia Twoje wymagania (domyślnie, zaplanowane uruchomienie zadania jest ustawione na **Ręcznie**, ale możesz chcieć wybrać inną opcję).

   Inne aplikacje Kaspersky mogą mieć inne domyślne zadania. Więcej informacji można znaleźć w dokumentacji dla konkretnej aplikacji.

   Upewnij się, że terminarz dla każdego zadania, które tworzysz, spełnia Twoje wymagania.

5. **Instalowanie Kaspersky Security for Mobile (opcjonalnie)**

   Jeśli planujesz zarządzać firmowymi urządzeniami mobilnymi, postępuj zgodnie z instrukcjami podanymi w pomocy dla Kaspersky Security for Mobile, aby uzyskać informacje o wdrożeniu Kaspersky Endpoint Security for Android.

6. **Tworzenie profili**

   Utwórz profil dla każdej aplikacji ręcznie lub (w przypadku Kaspersky Endpoint Security for Windows) poprzez Kreator wstępnej konfiguracji. Możesz użyć domyślnych ustawień profilu; możesz także zmodyfikować domyślne ustawienia profilu zgodnie ze swoimi potrzebami w dowolnym momencie.

7. **Sprawdzanie wyników**

   Upewnij się, że zdalna instalacja zakończyła się pomyślnie: masz profile i zadania dla każdej aplikacji, a te aplikacje są instalowane na zarządzanych urządzeniach.

Wyniki

Zakończenie scenariusza powoduje, że:

- Zostaną utworzone wszystkie wymagane profile i zadania dla wybranych aplikacji.
- Terminarze zadań zostaną skonfigurowane według Twoich potrzeb.
- Wybrane aplikacje zostaną zainstalowane lub zostanie zaplanowane ich zainstalowanie na wybranych urządzeniach klienckich.

Uzyskiwanie wtyczek dla aplikacji firmy Kaspersky

Aby zdalnie zainstalować aplikację Kaspersky, taką jak Kaspersky Endpoint Security for Windows, musisz pobrać wtyczkę zarządzającą dla aplikacji.

W celu pobrania wtyczki zarządzającej dla aplikacji Kaspersky:

1. W menu głównym przejdź do **Ustawienia konsoli → Wtyczki sieciowe**.
2. W otwartym oknie kliknij przycisk **Dodaj**.

   Zostanie wyświetlona lista dostępnych wtyczek.
3. Na liście dostępnych wtyczek wybierz wtyczkę, którą chcesz pobrać (na przykład, Kaspersky Endpoint Security 11 for Windows), klikając jej nazwę.

   Zostanie wyświetlona strona opisu wtyczki.
4. Na stronie opisu wtyczki kliknij **Zainstaluj wtyczkę**.
5. Po zakończeniu instalacji, kliknij **OK**.

   Wtyczka zarządzająca zostanie pobrana z domyślną konfiguracją i zostanie wyświetlona na liście wtyczek zarządzających.

Możesz dodać wtyczki i zaktualizować pobrane wtyczki z pliku. Możesz pobierać wtyczki do zarządzania i webowe wtyczki do zarządzania ze strony pomocy technicznej Kaspersky.

W celu pobrania lub zaktualizowania wtyczki z pliku:

1. W menu głównym przejdź do **Ustawienia konsoli → Wtyczki sieciowe**.
2. Wykonaj jedną z poniższych czynności:
   - Kliknij **Dodaj z pliku**, aby pobrać wtyczkę z pliku.
   - Kliknij **Aktualizuj z pliku**, aby pobrać aktualizację wtyczkę z pliku.
3. Określ plik i sygnaturę pliku.
4. Pobierz określone pliki.

   Wtyczka zarządzająca zostanie pobrana z pliku i zostanie wyświetlona na liście wtyczek zarządzających.

Pobieranie i tworzenie pakietów instalacyjnych dla aplikacji Kaspersky

Możesz utworzyć pakiety instalacyjne dla aplikacji firmy Kaspersky z serwerów Kaspersky, jeśli Serwer administracyjny ma dostęp do internetu.

W celu pobrania i utworzenia pakietu instalacyjnego dla aplikacji Kaspersky:

1. Wykonaj jedną z poniższych czynności:
   - W menu głównym przejdź do **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.
   - W menu głównym przejdź do **Operacje → Repozytoria → Pakiety instalacyjne**.

Możesz także przejrzeć powiadomienia o nowych pakietach dla aplikacji firmy Kaspersky na liście powiadomień ekranowych. Jeśli istnieją powiadomienia o nowym pakiecie, możesz kliknąć odnośnik obok powiadomienia i przejść do listy dostępnych pakietów instalacyjnych.

Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

3. W pierwszym kroku kreatora wybierz **Utwórz pakiet instalacyjny dla aplikacji Kaspersky**.

   Pojawi się lista pakietów instalacyjnych dostępnych na serwerach sieciowych Kaspersky. Lista zawiera pakiety instalacyjne tylko dla tych aplikacji, które są kompatybilne z bieżącą wersją Kaspersky Security Center.

4. Kliknij nazwę pakietu instalacyjnego, na przykład, Kaspersky Endpoint Security for Windows (11.1.0).

   Zostanie otwarte okno z informacjami o pakiecie instalacyjnym.

   > Możesz pobrać i używać pakietu instalacyjnego, który zawiera narzędzia kryptograficzne, które implementują silne szyfrowanie, jeśli jest to zgodne z obowiązującymi przepisami i regulacjami. Aby pobrać pakiet instalacyjny Kaspersky Endpoint Security for Windows potrzebny w Twojej organizacji, miej na uwadze ustawodawstwo kraju, w którym znajdują się urządzenia klienckie Twojej organizacji.

5. Przeczytaj informacje i kliknij przycisk **Pobierz i utwórz pakiet instalacyjny**.

   Jeśli pakiet dystrybucyjny nie może zostać przekonwertowany na pakiet instalacyjny, wyświetlany jest przycisk **Pobierz pakiet dystrybucyjny** zamiast **Pobierz i utwórz pakiet instalacyjny**.

   Rozpocznie się pobieranie pakietu instalacyjnego na Serwer administracyjny. Możesz zamknąć okno kreatora lub przejść do następnego kroku instrukcji. Jeśli zamkniesz okno kreatora, proces pobierania będzie kontynuowany w tle.

   Jeśli chcesz śledzić proces pobierania pakietu instalacyjnego:

   a. W menu głównym przejdź do **Operacje → Repozytoria → Pakiety instalacyjne → W toku ()**.

   b. Śledź proces działania w kolumnie **Postęp pobierania** oraz w kolumnie **Stan pobierania** tabeli.

   Po zakończeniu procesu pakiet instalacyjny zostanie dodany do listy na zakładce **Pobrano**. Jeśli proces pobierania zostanie zatrzymany, a stan pobierania przełączy się na **Zaakceptuj Umowę licencyjną**, kliknij nazwę pakietu instalacyjnego, a następnie przejdź do kolejnego kroku instrukcji.

   > Jeśli rozmiar danych znajdujących się w wybranym pakiecie dystrybucyjnym przekracza bieżące ograniczenie, zostanie wyświetlona wiadomość o błędzie. Możesz zmienić ograniczoną wartość, a następnie przejdź do tworzenia pakietu instalacyjnego.

6. Dla niektórych aplikacji Kaspersky, podczas pobierania wyświetlany jest przycisk **Pokaż Umowę licencyjną**. Jeśli przycisk jest wyświetlany, wykonaj następujące czynności:

   a. Kliknij przycisk **Pokaż Umowę licencyjną**, aby przeczytać Umowę licencyjną.

   b. Przeczytaj Umowę licencyjną, która zostanie wyświetlona na ekranie, i kliknij **Zaakceptuj**.

      Po zaakceptowaniu Umowy licencyjnej, proces pobierania będzie kontynuowany. Jeśli klikniesz **Odrzuć**, proces pobierania zostanie zatrzymany.

7. Po zakończeniu pobierania kliknij przycisk **Zamknij**.

Wybrany pakiet instalacyjny zostanie pobrany do folderu współdzielonego Serwera administracyjnego, do podfolderu Pakiety. Po pobraniu, pakiet instalacyjny jest wyświetlany na liście pakietów instalacyjnych.

Zmienianie ograniczenia rozmiaru danych niestandardowego pakietu instalacyjnego

Całkowity rozmiar danych wypakowanych podczas tworzenia niestandardowego pakietu instalacyjnego jest ograniczony. Domyślne ograniczenie to 1 GB.

Jeśli spróbujesz przesłać plik archiwum, który zawiera dane przekraczające bieżące ograniczenie, zostanie wyświetlony komunikat o błędzie. Konieczne może być zwiększenie tej wartości ograniczenia podczas tworzenia pakietów instalacyjnych z dużych pakietów dystrybucyjnych.

W celu zmiany wartości ograniczenia dla rozmiaru niestandardowego pakietu instalacyjnego:

1. Na urządzeniu Serwera administracyjnego uruchom wiersz poleceń z poziomu konta, które zostało użyte do zainstalowania Serwera administracyjnego.

2. Zmień bieżący katalog na folder instalacyjny Kaspersky Security Center (zwykle <dysk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. W zależności od rodzaju instalacji serwera administracyjnego, wprowadź jedno z poniższych poleceń, korzystając z uprawnień administratora:

   - Normalna instalacja lokalna:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <liczba bajtów>
     ```

   - Instalacja klastra trybu failover Kaspersky:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <liczba bajtów> --stp klfoc
     ```

   - Instalowanie klastra trybu failover Microsoft:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <liczba bajtów> --stp cluster
     ```

   Gdzie <liczba bajtów> to liczba bajtów w formacie szesnastkowym lub dziesiętnym.

   Na przykład, jeśli wymagany limit wynosi 2 GB, można określić wartość dziesiętną 2147483648 lub wartość szesnastkową 0x80000000. W takim przypadku w przypadku lokalnej instalacji Serwera administracyjnego możesz użyć następującego polecenia:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Ograniczenie rozmiaru danych niestandardowego pakietu instalacyjnego zostanie zmienione.

Pobieranie pakietów dystrybucyjnych dla aplikacji Kaspersky

W Kaspersky Security Center Web Console możesz pobrać i zapisać pakiety dystrybucyjne dla aplikacji firmy Kaspersky. Możesz użyć pakietów dystrybucyjnych do ręcznego zainstalowania aplikacji, bez użycia Kaspersky Security Center.

W celu pobrania i zapisania pakietów dystrybucyjnych dla aplikacji Kaspersky:

1. W menu głównym przejdź do **Operations** → **Kaspersky applications** → **Current application versions**.

   Zostanie otwarta lista dostępnych pakietów dystrybucyjnych, wtyczek i łat. Kaspersky Security Center wyświetla tylko te elementy, które są kompatybilne z jego bieżącą wersją.

2. Na liście kliknij nazwę pakietu, który chcesz pobrać.

   Zostanie otwarty opis pakietu.

3. Przeczytaj opis i kliknij przycisk **Pobierz i utwórz pakiet instalacyjny**.

   Jeśli pakiet dystrybucyjny nie może zostać przekonwertowany na pakiet instalacyjny, wyświetlany jest przycisk **Pobierz pakiet dystrybucyjny** zamiast **Pobierz i utwórz pakiet instalacyjny**.

   Rozpocznie się pobieranie pakietu instalacyjnego na Serwer administracyjny.

Wybrany pakiet instalacyjny lub dystrybucyjny zostanie pobrany do folderu współdzielonego Serwera administracyjnego, do podfolderu **Pakiety**. Po pobraniu, pakiet instalacyjny jest wyświetlany na liście pakietów instalacyjnych.

Sprawdzanie, czy Kaspersky Endpoint Security został pomyślnie wdrożony

W celu zapewnienia poprawnego zainstalowania aplikacji firmy Kaspersky, takich jak Kaspersky Endpoint Security:

1. Korzystając z Kaspersky Security Center Web Console, upewnij się, że posiadasz:

   - Zasada dla Kaspersky Endpoint Security i/lub innych aplikacji zabezpieczających, których używasz.
   - Zadania dla Kaspersky Endpoint Security for Windows: zadanie *Szybkie skanowanie* i zadanie *Zainstaluj aktualizację* (jeśli używasz Kaspersky Endpoint Security for Windows).
   - Zadania dla innych aplikacji zabezpieczających, których używasz.

2. Na jednym z zarządzanych urządzeń, wybranym dla instalacji, upewnij się, że:

   - Zainstalowany jest program Kaspersky Endpoint Security lub inna aplikacja zabezpieczająca firmy Kaspersky.
   - W Kaspersky Endpoint Security ustawienia Ochrony plików, Ochrony WWW i Ochrony poczty odpowiadają profilowi, który utworzyłeś dla tego urządzenia.
   - Usługa Kaspersky Endpoint Security może zostać zatrzymana i uruchomiona ręcznie.
   - Zadania grupowe mogą być zatrzymywane i uruchamiane ręcznie.

Tworzenie autonomicznych pakietów instalacyjnych

Ty oraz użytkownicy urządzeń w Twojej organizacji mogą używać autonomicznych pakietów instalacyjnych, aby ręcznie instalować aplikacje na urządzeniach.

Autonomiczny pakiet instalacyjny jest plikiem wykonywalnym (installer.exe), który można umieścić na serwerze sieciowym lub w folderze sieciowym, wysłać za pośrednictwem poczty elektronicznej lub przenieść na urządzenie klienckie w dowolny sposób. Na urządzeniu klienckim użytkownik może uruchomić otrzymany plik lokalnie, aby zainstalować aplikację bez udziału Kaspersky Security Center. Możesz tworzyć autonomiczne pakiety instalacyjne dla aplikacji Kaspersky i aplikacji innych firm na platformy Windows, macOS i Linux. Aby utworzyć autonomiczny pakiet instalacyjny dla aplikacji firmy trzeciej, należy utworzyć niestandardowy pakiet instalacyjny.

Upewnij się, że autonomiczny pakiet instalacyjny nie jest dostępny dla nieupoważnionych osób.

W celu utworzenia autonomicznego pakietu instalacyjnego:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź do **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.
   - W menu głównym przejdź do **Operacje → Repozytoria → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.

2. Na liście pakietów instalacyjnych wybierz pakiet instalacyjny i nad listą kliknij przycisk **Wdrażaj**.

3. Wybierz opcję **Przy użyciu pakietów autonomicznych**.

   Zostanie uruchomiony Kreator tworzenia autonomicznego pakietu instalacyjnego. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.

4. W pierwszym kroku kreatora, upewnij się, że opcja **Zainstaluj Agenta sieciowego wraz z aplikacją** jest włączona, jeśli chcesz zainstalować Agenta sieciowego wraz z wybraną aplikacją.

   Domyślnie opcja ta jest włączona. Zalecane jest włączenie tej opcji, jeśli nie jesteś pewien, czy Agent sieciowy jest zainstalowany na urządzeniu. Jeśli Agent sieciowy jest już zainstalowany na urządzeniu, po zainstalowaniu autonomicznego pakietu instalacyjnego wraz z Agentem sieciowym, Agent sieciowy zostanie zaktualizowany do nowszej wersji.

   Jeśli wyłączysz tę opcję, Agent sieciowy nie zostanie zainstalowany na urządzeniu, a urządzenie będzie niezarządzane.

   Jeśli autonomiczny pakiet instalacyjny dla wybranej aplikacji już istnieje na Serwerze administracyjnym, kreator poinformuje o tym fakcie. W tym przypadku powinieneś wybrać jedno z następujących działań:

   - **Utwórz autonomiczny pakiet instalacyjny**. Wybierz tę opcję, na przykład, jeśli chcesz utworzyć autonomiczny pakiet instalacyjny dla nowej wersji aplikacji oraz chcesz zachować autonomiczny pakiet instalacyjny, który utworzyłeś dla poprzedniej wersji aplikacji. Nowy autonomiczny pakiet instalacyjny zostanie umieszczony w innym folderze.
   - **Użyj istniejącego autonomicznego pakietu instalacyjnego**. Wybierz tę opcję, jeśli chcesz użyć istniejącego autonomicznego pakietu instalacyjnego. Proces tworzenia pakietu nie zostanie uruchomiony.
   - **Ponownie skompiluj istniejący autonomiczny pakiet instalacyjny**. Wybierz tę opcję, jeśli ponownie chcesz utworzyć autonomiczny pakiet instalacyjny dla tej samej aplikacji. Autonomiczny pakiet instalacyjny znajduje się w tym samym folderze.

5. Na stronie **Przenieś do listy zarządzanych urządzeń** kreatora domyślnie jest włączona opcja **Nie przenoś urządzeń**. Jeśli chcesz przenieść urządzenie klienckie do dowolnej grupy administracyjnej po zainstalowaniu Agenta sieciowego, pozostaw tę opcję włączoną.

   Jeśli chcesz przenieść urządzenie klienckie po instalacji Agenta sieciowego, wybierz opcję **Przenieś nieprzypisane urządzenia do tej grupy** i określ grupę administracyjną, do której chcesz przenieść urządzenie klienckie. Domyślnie, urządzenie zostanie przeniesione do grupy **Zarządzane urządzenia**.

6. W kolejnym kroku kreatora, po zakończeniu procesu tworzenia autonomicznego pakietu instalacyjnego, kliknij przycisk **ZAKOŃCZ**.

   Kreator tworzenia autonomicznego pakietu instalacyjnego zostanie zamknięty.

Autonomiczny pakiet instalacyjny jest tworzony i umieszczany w podfolderze Pkglnst folderu współdzielonego Serwera administracyjnego. Możesz przejrzeć listę pakietów autonomicznych, klikając przycisk **Wyświetl listę pakietów autonomicznych** nad listą pakietów instalacyjnych.

Przeglądanie listy autonomicznych pakietów instalacyjnych

Możesz przejrzeć listę autonomicznych pakietów instalacyjnych i właściwości każdego autonomicznego pakietu instalacyjnego.

W celu przejrzenia listy autonomicznych pakietów instalacyjnych dla wszystkich pakietów instalacyjnych:

Nad listą kliknij przycisk **Wyświetl listę pakietów autonomicznych**.

Na liście autonomicznych pakietów instalacyjnych ich właściwości są wyświetlane w następujący sposób:

- **Nazwa pakietu**. Nazwa autonomicznego pakietu instalacyjnego, który jest automatycznie tworzony jako nazwa aplikacji znajdującej się w pakiecie oraz wersja aplikacji.
- **Nazwa aplikacji**. Nazwa aplikacji znajdującej się w autonomicznym pakiecie instalacyjnym.
- **Wersja aplikacji**.
- **Nazwa pakietu instalacyjnego Agenta sieciowego**. Właściwość jest wyświetlana tylko wtedy, gdy Agent sieciowy znajduje się w autonomicznym pakiecie instalacyjnym.
- **Wersja Agenta sieciowego**. Właściwość jest wyświetlana tylko wtedy, gdy Agent sieciowy znajduje się w autonomicznym pakiecie instalacyjnym.
- **Rozmiar**. Rozmiar pliku w MB.
- **Grupa**. Nazwa grupy, do której urządzenie klienckie jest przenoszone po zainstalowaniu Agenta sieciowego.
- **Utworzono**. Data i godzina utworzenia autonomicznego pakietu instalacyjnego.
- **Zmodyfikowano**. Data i godzina modyfikacji autonomicznego pakietu instalacyjnego.
- **Ścieżka dostępu**. Pełna ścieżka do folderu, w którym znajduje się autonomiczny pakiet instalacyjny.
- **Adres internetowy**. Adres internetowy lokalizacji autonomicznego pakietu instalacyjnego.
- **Suma kontrolna pliku**. Właściwość jest używana do potwierdzenia, że autonomiczny pakiet instalacyjny nie został zmieniony przez osoby trzecie, a użytkownik posiada ten sam plik, który utworzyłeś i przesłałeś do użytkownika.

W celu przejrzenia listy autonomicznych pakietów instalacyjnych dla określonego pakietu instalacyjnego:

Wybierz pakiet instalacyjny na liście i, nad listą, kliknij przycisk **Wyświetl listę pakietów autonomicznych**.

Na liście autonomicznych pakietów instalacyjnych możesz zrobić co następuje:

- Opublikować autonomiczny pakiet instalacyjny na serwerze sieciowym, klikając przycisk **Publikuj**. Opublikowany autonomiczny pakiet instalacyjny jest dostępny do pobrania dla użytkowników, do których wysłałeś odnośnik do

autonomicznego pakietu instalacyjnego.

- Anulować publikację autonomicznego pakietu instalacyjnego na serwerze sieciowym, klikając przycisk **Cofnij publikowanie**. Nieopublikowany autonomiczny pakiet instalacyjny jest dostępny do pobrania tylko przez Ciebie i administratora.
- Pobrać autonomiczny pakiet instalacyjny na swoje urządzenie, klikając przycisk **Pobierz**.
- Wysłać e-mail z odnośnikiem do autonomicznego pakietu instalacyjnego, klikając przycisk **Wyślij przez e-mail**.
- Usunąć autonomiczny pakiet instalacyjny, klikając przycisk **Usuń**.

Tworzenie niestandardowego pakietu instalacyjnego

W celu wykonania następujących czynności możesz użyć niestandardowych pakietów instalacyjnych:

- Aby zainstalować dowolną aplikację (taką jak edytor tekstu) na urządzeniu klienckim, na przykład, przy użyciu zadania.
- Aby utworzyć autonomiczny pakiet instalacyjny.

Niestandardowy pakiet instalacyjny to folder z zestawem plików. Źródło utworzenia niestandardowego pakietu instalacyjnego to *plik archiwum*. Plik archiwum zawiera plik lub pliki, które muszą znajdować się w niestandardowym pakiecie instalacyjnym. Podczas tworzenia niestandardowego pakietu instalacyjnego możesz określić parametry wiersza poleceń, na przykład, aby zainstalować aplikację w trybie cichym.

Jeśli masz aktywny klucz licencyjny dla funkcji Zarządzanie lukami i poprawkami (VAPM), możesz przekonwertować domyślne ustawienia instalacji dla odpowiedniego niestandardowego pakietu instalacyjnego i użyć wartości zalecanych przez ekspertów z firmy Kaspersky. Ustawienia są automatycznie konwertowane podczas tworzenia niestandardowego pakietu instalacyjnego tylko wtedy, gdy odpowiedni plik wykonywalny znajduje się w bazie danych aplikacji firm trzecich Kaspersky.

W celu utworzenia niestandardowego pakietu instalacyjnego:

1. Wykonaj jedną z poniższych czynności:
   - W menu głównym przejdź do **Wykrywanie i wdrażanie → Wdrażanie i przypisywanie → Pakiety instalacyjne**.
   - W menu głównym przejdź do **Operacje → Repozytoria → Pakiety instalacyjne**.

   Zostanie wyświetlona lista pakietów instalacyjnych dostępnych na Serwerze administracyjnym.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego pakietu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. W pierwszym kroku kreatora wybierz **Utwórz pakiet instalacyjny z pliku**.
4. W kolejnym kroku kreatora określ nazwę pakietu i kliknij przycisk **Przeglądaj**.

   Zostanie otwarte standardowe okno **Otwórz** w przeglądarce, aby pomóc w wybraniu pliku do utworzenia pakietu instalacyjnego.

5. Wybierz plik archiwum znajdujący się na dostępnych dyskach.

   Możesz przesłać plik archiwum ZIP, CAB, TAR lub TAR.GZ. Nie jest możliwe utworzenie pakietu instalacyjnego z pliku SFX (samorozpakowujące się archiwum).

   > Jeśli chcesz, aby ustawienia zostały przekonwertowane podczas instalacji pakietu, upewnij się, że pole wyboru **Konwertuj ustawienia na zalecane wartości dla aplikacji rozpoznawanych przez Kaspersky Security Center po zakończeniu pracy kreatora** jest zaznaczone, a następnie kliknij **Dalej**.

   Rozpocznie się przesyłanie pliku na Serwer administracyjny Kaspersky Security Center.

   > Jeśli włączono korzystanie z zalecanych ustawień instalacji, Kaspersky Security Center 14.2 sprawdzi, czy plik wykonywalny znajduje się w bazie danych aplikacji firm trzecich Kaspersky. Jeśli sprawdzenie się powiedzie, otrzymasz powiadomienie informujące, że plik został rozpoznany. Ustawienia są konwertowane i tworzony jest niestandardowy pakiet instalacyjny. Dalsze działania nie są wymagane. W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

6. W kolejnym kroku kreatora wybierz plik (z listy plików, które są wypakowywane z wybranego pliku archiwum) i określ parametry wiersza poleceń pliku wykonywalnego.

   Możesz określić parametry wiersza poleceń, aby zainstalować aplikację z pakietu instalacyjnego w trybie cichym. Określanie parametrów wiersza poleceń jest opcjonalne.

   Zostanie uruchomiony proces tworzenia pakietu instalacyjnego.

   Kreator informuje, gdy proces zostanie zakończony.

   Jeśli pakiet instalacyjny nie zostanie utworzony, zostanie wyświetlona odpowiednia wiadomość.

7. W celu zakończenia działania kreatora kliknij przycisk **Zakończ**.

Pakiet instalacyjny, który utworzyłeś, zostanie pobrany do podfolderu Packages folderu współdzielonego Serwera administracyjnego. Po pobraniu, pakiet instalacyjny pojawi się na liście pakietów instalacyjnych.

Na liście pakietów instalacyjnych dostępnych na Serwerze administracyjnym, klikając odnośnik z nazwą niestandardowego pakietu instalacyjnego, możesz:

- Wyświetl następujące właściwości pakietu instalacyjnego:
  - **Nazwa**. Nazwa niestandardowego pakietu instalacyjnego.
  - **Źródło**. Nazwa producenta aplikacji.
  - **Aplikacja**. Nazwa aplikacji spakowanej w niestandardowy pakiet instalacyjny.
  - **Wersja**. Wersja aplikacji.
  - **Język**. Wersja językowa aplikacji spakowanej w niestandardowy pakiet instalacyjny.
  - **Rozmiar (MB)**. Rozmiar pakietu instalacyjnego.
  - **System operacyjny**. Typ systemu operacyjnego, dla którego przeznaczony jest pakiet instalacyjny.
  - **Utworzono**. Data utworzenia pakietu instalacyjnego.
  - **Zmodyfikowano**. Data modyfikacji pakietu instalacyjnego.

- **Typ**. Typ pakietu instalacyjnego.

- Zmień nazwę pakietu instalacyjnego i parametry wiersza poleceń. Ta funkcja jest dostępna tylko dla pakietów, które nie są tworzone w oparciu o aplikacje Kaspersky.

Jeśli dla procesu tworzenia pakietu niestandardowego przekonwertowałeś ustawienia instalacji pakietu na zalecane wartości, na zakładce **Ustawienia** we właściwościach niestandardowego pakietu instalacyjnego mogą pojawić się dwie dodatkowe sekcje: **Ustawienia** i **Procedura instalacji**.

Sekcja **Ustawienia** zawiera następujące właściwości, wyświetlane w tabeli:

- **Nazwa**. W tej kolumnie wyświetlana jest nazwa przypisana do parametru instalacji.

- **Typ**. Ta kolumna pokazuje typ parametru instalacji.

- **Wartość**. Ta kolumna pokazuje typ danych zdefiniowany przez parametr instalacji (Boolowski, Ścieżka pliku, Liczbowy, Ścieżka lub Ciąg znaków).

Sekcja **Procedura instalacji** zawiera tabelę opisującą następujące właściwości aktualizacji zawartej w niestandardowym pakiecie instalacyjnym:

- **Nazwa**. Nazwa aktualizacji.

- **Opis**. Opis aplikacji.

- **Źródło**. Źródło aktualizacji, czyli czy została ona wydana przez firmę Microsoft, czy przez inną niezależną firmę.

- **Typ**. Rodzaj aktualizacji, czyli czy jest przeznaczona dla sterownika czy aplikacji.

- **Kategoria**. Kategoria Windows Server Update Services (WSUS) wyświetlana dla aktualizacji firmy Microsoft (aktualizacje krytyczne, aktualizacje definicji, sterowniki, pakiety funkcji, aktualizacje zabezpieczeń, dodatki Service Pack, narzędzia, pakiety zbiorcze aktualizacji, aktualizacje lub uaktualnienie).

- **Poziom ważności zgodnie z MSRC**. Istotność aktualizacji określona przez Microsoft Security Response Center (MSRC).

- **Priorytet**. Istotność aktualizacji określona przez Kaspersky.

- **Poziom ważności poprawki (dla poprawek przeznaczonych dla aplikacji Kaspersky)**. Istotność poprawki, jeśli jest ona przeznaczona dla aplikacji Kaspersky.

- **Artykuł**. Identyfikator (ID) artykułu w bazie wiedzy opisującego aktualizację.

- **Biuletyn**. Identyfikator biuletynu zabezpieczeń opisującego aktualizację.

- **Nie jest przeznaczony do instalacji**. Wyświetla, czy aktualizacja ma stan Nieprzypisane do instalacji.

- **Do zainstalowania**. Wyświetla, czy aktualizacja ma stan Do zainstalowania.

- **Instalowanie**. Wyświetla, czy aktualizacja ma stan Instalowanie.

- **Zainstalowana**. Wyświetla, czy aktualizacja ma stan Zainstalowana.

- **Niepowodzenie**. Wyświetla, czy aktualizacja ma stan Niepowodzenie.

- **Wymagane ponowne uruchomienie**. Wyświetla, czy aktualizacja ma stan Wymagane ponowne uruchomienie.
- **Zarejestrowano**. Wyświetla datę i godzinę rejestracji aktualizacji.
- **Instalacja w trybie interaktywnym**. Wyświetla, czy aktualizacja wymaga interakcji z użytkownikiem podczas instalacji.
- **Odwołano**. Wyświetla datę i godzinę odwołania aktualizacji.
- **Stan zatwierdzenia aktualizacji**. Wyświetla, czy aktualizacja została zatwierdzona do instalacji.
- **Wersja**. Wyświetla aktualny numer wersji aktualizacji.
- **Identyfikator aktualizacji**. Wyświetla identyfikator aktualizacji.
- **Wersja aplikacji**. Wyświetla numer wersji, do jakiej aplikacja zostanie zaktualizowana.
- **Zastąpiono**. Wyświetla inne aktualizacje, które mogą zastąpić aktualizację.
- **Zastępowanie**. Wyświetla inne aktualizacje, które mogą zostać zastąpione przez aktualizację.
- **Należy zaakceptować warunki Umowy licencyjnej**. Wyświetla, czy aktualizacja wymaga akceptacji warunków Umowy licencyjnej(EULA).
- **Producent**. Wyświetla nazwę producenta aktualizacji.
- **Rodzina aplikacji**. Wyświetla nazwę rodziny aplikacji, do której należy aktualizacja.
- **Aplikacja**. Wyświetla nazwę aplikacji, do której należy aktualizacja.
- **Język**. Wyświetla język aktualizacji.
- **Nie przypisano do instalacji (nowa wersja)**. Wyświetla, czy aktualizacja ma stan Nie przypisano do instalacji (nowa wersja).
- **Wymaga instalacji wymagań wstępnych**. Wyświetla, czy aktualizacja ma stan Wymaga instalacji wymagań wstępnych.
- **Tryb pobierania**. Wyświetla tryb pobierania aktualizacji.
- **To aktualizacja**. Wyświetla, czy aktualizacja jest poprawką.
- **Nie zainstalowano**. Wyświetla, czy aktualizacja ma stan Nie zainstalowano.

Rozsyłanie pakietów instalacyjnych na podrzędne Serwery administracyjne

Kaspersky Security Center umożliwia tworzenie pakietów instalacyjnych dla aplikacji firmy Kaspersky i aplikacji firm trzecich, a także dystrybucję pakietów instalacyjnych na urządzeniach klienckich i instalowanie aplikacji z pakietów. Aby zoptymalizować obciążenie podstawowego Serwera administracyjnego, możesz rozesłać pakiety instalacyjne do pomocniczych Serwerów administracyjnych. Serwery pomocnicze przesyłają pakiety do urządzeń klienckich, a następnie można przeprowadzić zdalną instalację aplikacji na urządzeniach klienckich.

W celu rozesłania pakietów instalacyjnych na podrzędne Serwery administracyjne:

1. Upewnij się, że drugorzędne Serwery administracyjne są połączone z głównym Serwerem administracyjnym.

2. W menu głównym przejdź do **Urządzenia** → **Zadania**.

   Zostanie wyświetlona lista zadań.

3. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

4. Na stronie **Nowe zadanie**, z listy rozwijalnej **Aplikacja** wybierz **Kaspersky Security Center**. Następnie z listy rozwijanej **Typ zadania** wybierz opcję **Rozsyłanie pakietu instalacyjnego**, a następnie określ nazwę zadania.

5. Na stronie **Zakres zadania** wybierz urządzenia, do których zadanie jest przypisane w jeden z następujących sposobów:

   - Jeśli chcesz utworzyć zadanie dla wszystkich pomocniczych Serwerów administracyjnych w określonej grupie administracyjnej, wybierz tę grupę, a następnie utwórz dla niej zadanie grupowe.

   - Jeśli chcesz utworzyć zadanie dla określonych pomocniczych Serwerów administracyjnych, wybierz te Serwery, a następnie utwórz dla nich zadanie.

6. Na stronie **Rozesłane pakiety instalacyjne** wybierz pakiety instalacyjne, które mają zostać skopiowane na dodatkowe Serwery administracyjne.

7. Określ konto, aby uruchomić zadanie *Dystrybucja pakietu instalacyjnego w* ramach tego konta. Możesz użyć swojego konta i pozostawić włączoną opcję **Konto domyślne**. Alternatywnie można określić, że zadanie powinno być uruchamiane na innym koncie, które ma niezbędne prawa dostępu. Aby to zrobić, wybierz opcję **Określ konto**, a następnie wprowadź poświadczenia tego konta.

8. Na stronie **Zakończ tworzenie zadania** możesz włączyć opcję **Otwórz szczegóły zadania po jego utworzeniu**, aby otworzyć okno właściwości zadania i zmodyfikować domyślne ustawienia zadania. W przeciwnym razie możesz skonfigurować ustawienia zadania później, w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie utworzone w celu dystrybucji pakietów instalacyjnych na drugorzędne Serwery administracyjne jest wyświetlane na liście zadań.

10. Możesz uruchomić zadanie ręcznie lub poczekać na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania wybrane pakiety instalacyjne są kopiowane na określone pomocnicze Serwery administracyjne.

Opcje ręcznej instalacji aplikacji

Możesz zainstalować Agenta sieciowego na urządzeniach lokalnie bez korzystania z Kaspersky Security Center Cloud Console. W tym celu utwórz autonomiczny pakiet instalacyjny dla Agenta sieciowego zgodnie z opisem w następującym temacie: Tworzenie autonomicznych pakietów instalacyjnych. Przenieś pakiet na urządzenie klienckie i zainstaluj go. Po zakończeniu instalacji Agenta sieciowego możesz używać urządzenia jako punktu dystrybucji.

Instalowanie aplikacji przy pomocy zadania zdalnej instalacji

Kaspersky Security Center umożliwia zdalne instalowanie aplikacji na urządzeniach przy użyciu zadań zdalnej instalacji. Te zadania są tworzone i przydzielane do urządzeń za pośrednictwem dedykowanego kreatora. W celu szybkiego i łatwego przypisywania zadań do urządzeń, należy wskazać urządzenia w oknie kreatora w jeden z następujących sposobów:

- **Wybierz urządzenia wykryte w sieci przez Serwer administracyjny**. W tym przypadku zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.
- **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**. Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.
- **Przypisz zadanie do wyboru urządzeń**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonym wyborze. Możesz określić domyślny wybór lub niestandardowy wybór, który utworzyłeś.
- **Przypisz zadanie do grupy administracyjnej**. W tym przypadku zadanie jest przypisywane do urządzeń znajdujących się we wcześniej utworzonej grupie administracyjnej.

Aby zdalna instalacja została poprawnie przeprowadzona na urządzeniu, na którym nie został zainstalowany Agent sieciowy, muszą być otwarte następujące porty: a) TCP 139 i 445; b) UDP 137 i 138. Domyślnie porty te są otwarte dla wszystkich urządzeń z domeny. Porty te są otwierane automatycznie przy użyciu narzędzia do przygotowania zdalnej instalacji.

Instalowanie aplikacji na określonych urządzeniach

Ta sekcja zawiera informacje na temat zdalnej instalacji aplikacji na grupie administracyjnej, urządzeniach o określonych adresach IP lub wybranych zarządzanych urządzeniach.

W celu zainstalowania aplikacji na określonych urządzeniach:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie urządzenia.
2. W menu głównym przejdź do **Urządzenia** → **Zadania**.
3. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
4. W polu **Typ zadania** wybierz **Zdalna instalacja aplikacji**.
5. Wybierz jedną z następujących opcji:

   - Przypisz zadanie do grupy administracyjnej

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.
   - Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy

Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

- **Przypisz zadanie do wyboru urządzeń**

  Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

  Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

6. Postępuj zgodnie z instrukcjami kreatora.

   Kreator nowych zadania tworzy zadanie zdalnej instalacji wybranej w Kreatorze aplikacji na określonych urządzeniach. Jeśli wybrano opcję **Przypisz zadanie do grupy administracyjnej**, zadanie jest zadaniem grupowym.

7. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji wybrana aplikacja zostanie zainstalowana na określonych urządzeniach.

Instalowanie aplikacji przy użyciu zasad grupy Active Directory

Kaspersky Security Center pozwala na instalowanie aplikacji Kaspersky na zarządzanych urządzeniach przy użyciu zasad grupy Active Directory.

Możesz zainstalować aplikacje, korzystając z zasad grupy Active Directory jedynie przy pomocy pakietów instalacyjnych, które zawierają Agenta sieciowego.

W celu zainstalowania aplikacji przy użyciu profili grupy Active Directory:

1. Uruchom Kreator wdrażania ochrony. Postępuj zgodnie z instrukcjami kreatora.
2. Na stronie **Ustawienia zadania zdalnej instalacji** Kreatora wdrażania ochrony włącz opcję **Przypisz pakiet instalacyjny do zasad grupy Active Directory**.
3. Na stronie **Wybierz konta w celu uzyskania dostępu do urządzeń** wybierz opcję **Konto wymagane (Agent sieciowy nie jest używany)**.
4. Dodaj konto z uprawnieniami administratora na urządzeniu, na którym jest zainstalowany program Kaspersky Security Center, lub konto, które należy do grupy domeny Twórcy-właściciele zasad grupy.
5. Nadaj wybranemu kontu następujące uprawnienia:
   a. Przejdź do **Panel sterowania** → **Narzędzia administracyjne** i otwórz **Zarządzanie zasadami grupy**.
   b. Kliknij węzeł z żądaną domeną.

c. Kliknij sekcję **Delegowanie**.

d. Na liście rozwijanej **Uprawnienia** wybierz opcję **Połącz obiekty zasad grupy**.

e. Kliknij **Dodaj**.

f. W otwartym oknie **Wybierz Użytkownika, Komputer lub Grupę** wybierz żądane konto.

g. Kliknij **OK**, aby zamknąć okno **Wybierz Użytkownika, Komputer lub Grupę**.

h. Na liście **Grupy i użytkownicy** wybierz konto, które zostało dodane, a następnie kliknij **Zaawansowane** → **Zaawansowane**.

i. Na liście **Wpisy uprawnień** kliknij dwukrotnie konto, które tyle co dodałeś.

j. Nadaj następujące uprawnienia:

- **Utwórz obiekty grupy**
- **Usuń obiekty grupy**
- **Utwórz obiekty kontenera zasad grupy**
- **Usuń obiekty kontenera zasad grupy**

k. Kliknij **OK**, aby zachować zmiany.

6. Określ inne ustawienia, postępując zgodnie z instrukcjami kreatora.

7. Uruchom utworzone zadanie zdalnej instalacji ręcznie lub zaczekaj na jego uruchomienie zgodne z terminarzem.

Rozpocznie się następująca sekwencja zdalnej instalacji:

1. Po uruchomieniu zadania, w każdej domenie, do której należą urządzenia klienckie z określonego zbioru, zostaną utworzone następujące obiekty:

   - Obiekt zasad grupy (GPO) o nazwie **Kaspersky_AK{GUID}**.
   - Grupa bezpieczeństwa, która odpowiada GPO. Ta grupa bezpieczeństwa zawiera urządzenia klienckie objęte zadaniem. Zawartość grupy bezpieczeństwa określa zakres GPO.

2. Kaspersky Security Center instaluje wybrane aplikacje firmy Kaspersky na urządzeniach klienckich bezpośrednio z sieciowego folderu współdzielonego Share. W folderze instalacyjnym Kaspersky Security Center zostanie utworzony pomocniczy podfolder, zawierający plik .msi potrzebny do zainstalowania aplikacji.

3. Po dodaniu nowych urządzeń do obszaru zadania, są one dodawane do grupy bezpieczeństwa podczas kolejnego uruchomienia zadania. Jeśli w terminarzu uruchamiania zadania wybrana jest opcja **Uruchom pominięte zadania**, urządzenia są dodawane do grupy zabezpieczeń od razu.

4. Po usunięciu urządzeń z obszaru zadania, są one usuwane z grupy zabezpieczeń podczas kolejnego uruchomienia zadania.

5. Po usunięciu zadania z Active Directory, usuwany jest GPO, odnośnik do GPO oraz odpowiadająca mu grupa zabezpieczeń.

Jeżeli chcesz zastosować inny schemat instalacji przy użyciu Active Directory, możesz ręcznie skonfigurować żądane ustawienia. Na przykład, może to być wymagane w następujących wypadkach:

- Jeśli administrator ochrony antywirusowej nie ma uprawnień do wprowadzania zmian w Active Directory pewnych domen
- Jeśli oryginalny pakiet instalacyjny musi być przechowywany w oddzielnym zasobie sieciowym
- Jeśli konieczne jest połączenie GPO z określonymi jednostkami Active Directory

Dostępne są następujące opcje korzystania z alternatywnego scenariusza instalacji poprzez Active Directory:

- W przypadku, gdy instalacja musi być przeprowadzona bezpośrednio z folderu współdzielonego Kaspersky Security Center, we właściwościach GPO musisz określić plik msi zlokalizowany w podfolderze exec folderu pakietu instalacyjnego żądanej aplikacji.
- Jeżeli pakiet instalacyjny ma znajdować się w innym zasobie sieciowym, skopiuj do niego całą zawartość foldera exec. Jest to konieczne, gdyż oprócz pliku z rozszerzeniem .msi folder zawiera pliki konfiguracyjne wygenerowane podczas tworzenia pakietu. W celu zainstalowania aplikacji wraz z kluczem licencyjnym, skopiuj do tego folderu także plik klucza.

Instalowanie aplikacji na podrzędnych Serwerach administracyjnych

W celu zainstalowania aplikacji na podrzędnych Serwerach administracyjnych:

1. Nawiąż połączenie z Serwerem administracyjnym kontrolującym odpowiednie podrzędne Serwery administracyjne.
2. Upewnij się, że pakiet instalacyjny dla instalowanej aplikacji znajduje się na każdym z wybranych podrzędnych Serwerów administracyjnych. Jeśli nie możesz znaleźć pakietu instalacyjnego na żadnym z serwerów podrzędnych, dystrybuuj go. W tym celu utwórz zadanie z typem zadania **Rozsyłanie pakietu instalacyjnego**.
3. Utwórz zadanie zdalnej instalacji aplikacji na podrzędnych Serwerach administracyjnych. Wybierz typ zadania **Zdalna instalacja aplikacji na podrzędnym Serwerze administracyjnym**.

   Kreator nowego zadania tworzy zadanie zdalnej instalacji aplikacji wybranej w Kreatorze na określonych podrzędnych Serwerach administracyjnych.
4. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej instalacji wybrana aplikacja zostanie zainstalowana na podrzędnych Serwerach administracyjnych.

Określanie ustawień zdalnej instalacji na urządzeniach z systemem Unix

Podczas instalowania aplikacji na urządzeniu z systemem UNIX przy użyciu zadania instalacji zdalnej można określić ustawienia zadania specyficzne dla systemu Unix. Te ustawienia są dostępne we właściwościach zadania po jego utworzeniu.

W celu określenia ustawień specyficznych dla systemu Unix dla zadania zdalnej instalacji:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.

2. Kliknij nazwę zadania zdalnej instalacji, dla którego chcesz określić ustawienia specyficzne dla systemu Unix.

   Zostanie otwarte okno właściwości zadania.

3. Przejdź do **Ustawienia aplikacji** → **Ustawienia specyficzne dla systemu Unix**.

4. Określ następujące ustawienia:

   - **Ustaw hasło do konta root (tylko do wdrożenia przez SSH)**

     Jeśli polecenie `sudo` nie może być używane na urządzeniu docelowym bez określenia hasła, wybierz tę opcję, a następnie określ hasło dla konta root. Kaspersky Security Center przesyła hasło w postaci zaszyfrowanej na urządzenie docelowe, odszyfrowuje hasło, a następnie rozpoczyna procedurę instalacji w imieniu konta root z określonym hasłem.

     Kaspersky Security Center nie używa konta ani określonego hasła do tworzenia połączenia SSH.

   - **Określ ścieżkę do folderu tymczasowego z uprawnieniami do wykonywania na urządzeniu docelowym (tylko do wdrożenia przez SSH)**

     Jeśli katalog /tmp na urządzeniu docelowym nie ma uprawnień do wykonywania, wybierz tę opcję, a następnie określ ścieżkę do katalogu z uprawnieniem do wykonywania. Kaspersky Security Center używa określonego katalogu jako katalogu tymczasowego w celu uzyskania dostępu przez SSH. Aplikacja umieszcza pakiet instalacyjny w katalogu i uruchamia procedurę instalacji.

5. Kliknij przycisk **Zapisz**.

   Określone ustawienia zadania zostaną zapisane.

Zarządzanie urządzeniami mobilnymi

Zarządzanie ochroną urządzeń mobilnych poprzez Kaspersky Security Center jest realizowane przy użyciu funkcji Zarządzanie urządzeniami mobilnymi, która wymaga dedykowanej licencji. Jeśli zamierzasz zarządzać urządzeniami mobilnymi należącymi do pracowników Twojej organizacji, włącz i skonfigurować Zarządzanie urządzeniami mobilnymi.

Zarządzanie urządzeniami mobilnymi umożliwia zarządzanie urządzeniami z systemem Android należącymi do pracowników. Ochronę zapewnia aplikacja mobilna Kaspersky Endpoint Security for Android zainstalowana na urządzeniach. Ta aplikacja mobilna zapewnia ochronę urządzeń mobilnych przed zagrożeniami internetowymi, wirusami i innymi programami stanowiącymi zagrożenie. W celu scentralizowanego zarządzania przez konsolę Kaspersky Security Center Web Console musisz zainstalować następujące wtyczki do zarządzania siecią na urządzeniu, na którym jest zainstalowany Kaspersky Security Center Web Console:

- Wtyczka Kaspersky Security for Mobile
- Wtyczka Kaspersky Endpoint Security for Android

Aby uzyskać informacje na temat wdrażania ochrony i zarządzania urządzeniami mobilnymi, zapoznaj się z pomocą dla Kaspersky Security for Mobile.

Modyfikowanie ustawień Zarządzania urządzeniami mobilnymi w Kaspersky Security Center Web Console

W celu zmodyfikowania ustawień Zarządzania urządzeniami mobilnymi:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Porty dodatkowe**.

3. Zmodyfikuj odpowiednie ustawienia:

   - **Otwórz port dla urządzeń mobilnych**

     Jeśli ta opcja jest włączona, port dla urządzeń mobilnych zostanie otwarty na Serwerze administracyjnym.

     Port dla urządzeń mobilnych może zostać użyty tylko wtedy, gdy zainstalowany jest komponent Zarządzanie urządzeniami mobilnymi.

     Jeśli ta opcja jest wyłączona, port dla urządzeń mobilnych na Serwerze administracyjnym nie będzie używany.

     Domyślnie opcja ta jest wyłączona.

   - **Port do synchronizacji urządzeń mobilnych**

     Numer portu używanego dla połączenia nawiązywanego między urządzeniami mobilnymi a Serwerem administracyjnym. Domyślny numer portu to 13292.

     Używany jest system dziesiętny.

   - **Port do aktywacji urządzeń mobilnych**

     Port do łączenia Kaspersky Endpoint Security for Android z serwerami aktywacji Kaspersky.

     Domyślny numer portu to 17100.

4. Kliknij przycisk **Zapisz**.

Urządzenia mobilne mogą nawiązywać połączenie z Serwerem administracyjnym.

Zastępowanie aplikacji zabezpieczających firm trzecich

Instalacja aplikacji zabezpieczających firmy Kaspersky poprzez Kaspersky Security Center może wymagać usunięcia oprogramowania firmy trzeciej niekompatybilnego z instalowaną aplikacją. Kaspersky Security Center oferuje kilka sposobów usunięcia aplikacji firm trzecich.

Usuwanie niekompatybilnych aplikacji przy użyciu instalatora

Ta opcja jest dostępna tylko w Konsoli administracyjnej opartej na konsoli Microsoft Management Console.

Metoda instalatora dotycząca usuwania niekompatybilnych aplikacji jest obsługiwana przez różne typy instalacji. Przed zainstalowaniem aplikacji zabezpieczającej wszystkie niekompatybilne aplikacje są usuwane automatycznie, jeśli w oknie właściwości pakietu instalacyjnego tej aplikacji zabezpieczającej (sekcja **Niekompatybilne aplikacje**) wybrano opcję **Automatycznie odinstaluj niekompatybilne aplikacje**.

Usuwanie niekompatybilnych aplikacji podczas konfigurowania zdalnej instalacji aplikacji

Możesz włączyć opcję **Automatycznie odinstaluj niekompatybilne aplikacje**, gdy konfigurujesz zdalną instalację aplikacji zabezpieczającej. W Konsoli administracyjnej opartej na Microsoft Management Console (MMC) ta opcja jest dostępna w kreatorze zdalnej instalacji. W Kaspersky Security Center Web Console tę opcję można znaleźć w kreatorze wdrażania ochrony. Jeśli ta opcja jest włączona, Kaspersky Security Center usunie niekompatybilne aplikacje przed zainstalowaniem aplikacji zabezpieczającej na zarządzanym urządzeniu.

Dostępne instrukcje:

- Konsola administracyjna: Instalowanie aplikacji przy pomocy kreatora zdalnej instalacji
- Kaspersky Security Center Web Console: Usuwanie niekompatybilnych aplikacji przed instalacją

Dezinstalowanie niekompatybilnych aplikacji przy użyciu dedykowanego zadania

Aby usunąć niekompatybilne aplikacje, użyj zadania **Zdalna dezinstalacja aplikacji**. Zadanie to powinno być uruchomione przed zadaniem instalacji aplikacji zabezpieczającej. Na przykład, w zadaniu instalacji możesz wybrać opcję terminarza **Po zakończeniu wykonywania innego zadania**, gdzie inne zadanie to **Zdalna dezinstalacja aplikacji**.

Ta metoda dezinstalacji jest przydatna, jeśli instalator aplikacji zabezpieczającej nie może skutecznie usunąć niekompatybilnej aplikacji.

Instrukcje dotyczące Konsoli administracyjnej: Tworzenie zadania.

Wykrywanie urządzeń w sieci

Ta sekcja opisuje wyszukiwanie i wykrywanie urządzeń w sieci.

Kaspersky Security Center umożliwia wyszukiwanie urządzeń w oparciu o określone kryteria. Wyniki wyszukiwania możesz zapisać do pliku tekstowego.

Opcja wyszukiwania i wykrywania pozwala znaleźć następujące urządzenia:

- Zarządzane urządzenia w grupach administracyjnych Serwera administracyjnego Kaspersky Security Center i jego podrzędnych Serwerów administracyjnych.
- Urządzenia nieprzypisane zarządzane przez Serwer administracyjny Kaspersky Security Center i jego podrzędne Serwery administracyjne.

Scenariusz: Wykrywanie urządzeń w sieci

Przed zainstalowaniem aplikacji zabezpieczających musisz przeprowadzić wykrywanie urządzeń. Serwer administracyjny otrzymuje informacje o wykrytych urządzeniach i umożliwia zarządzanie urządzeniami za pomocą profili. Do aktualizacji listy urządzeń dostępnych w sieci potrzebne są regularne ankiety sieciowe.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB1 jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Użyj następującego polecenia: `Get-SmbServerConfiguration | select EnableSMB1Protocol`

Wykrywanie urządzeń sieciowych przebiega w następujących krokach:

1. **Odkryj urządzenia**

   Kreator wstępnej konfiguracji poprowadzi Cię przez wstępne wyszukiwanie urządzeń i pomoże w odnalezieniu urządzeń w sieci, takich jak komputery, tablety i telefony komórkowe. Możesz także ręcznie przeprowadzić wykrywanie urządzeń.

2. **Skonfiguruj zaplanowane ankiety**

   Zdecyduj, których typów przeszukiwania chcesz używać regularnie. Włącz żądane typy i skonfiguruj harmonogram ankiety według własnego uznania. Możesz zapoznać się z zaleceniami dotyczącymi częstotliwości odpytywania sieci.

3. **(Opcjonalnie) Skonfiguruj reguły dodawania wykrytych urządzeń do grup administracyjnych**

   Jeśli nowe urządzenia pojawią się w Twojej sieci, zostaną wykryte podczas regularnych przeszukiwań i zostaną automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**. Możesz skonfigurować reguły przenoszenia urządzeń, aby zautomatyzować przydzielanie urządzeń do grupy **Zarządzane urządzenia**. Możesz także skonfigurować reguły zatrzymania.

   Jeśli pominiesz krok 3, nowo wykryte urządzenia zostaną przydzielone do grupy **Urządzenia nieprzypisane**. Jeśli chcesz, możesz ręcznie przenieść te urządzenia do grupy **Zarządzane urządzenia**. Jeśli ręcznie przeniesiesz te urządzenia do grupy **Zarządzane urządzenia**, możesz przeanalizować informacje o każdym urządzeniu i zdecydować, czy chcesz przenieść je do grupy administracyjnej i do jakiej grupy.

Wyniki

Zakończenie scenariusza powoduje, że:

- Serwer administracyjny Kaspersky Security Center wykrywa urządzenia, które znajdują się w sieci, i zapewnia informacje o nich.
- Przyszłe przeszukiwania zostają skonfigurowane i przeprowadzone zgodnie z określonym terminarzem.
- Nowo wykryte urządzenia zostaną rozmieszczone zgodnie ze skonfigurowanymi regułami (lub jeśli nie ma skonfigurowanych reguł, urządzenia pozostają w grupie **Urządzenia nieprzypisane**).

Wykrywanie urządzeń

Ta sekcja opisuje typy wykrywania urządzeń dostępne w Kaspersky Security Center i oferuje informacje dotyczące korzystania z każdego typu.

Serwer administracyjny otrzymuje informacje o strukturze sieci i urządzeń w tej sieci poprzez regularne przeszukiwanie. Informacje są zapisywane w bazie danych Serwera administracyjnego. Serwer administracyjny może wykorzystywać następujące typy przeszukiwania:

- **Przeszukiwanie sieci Windows**. Serwer administracyjny może wykonywać dwa rodzaje przeszukiwań sieci Windows: szybkie i pełne. Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych. Podczas pełnego przeszukiwania wymaganych jest więcej informacji z urządzenia klienckiego, takich jak: nazwa systemu operacyjnego, adres IP, nazwa DNS, nazwa NetBIOS. Domyślnie włączone są oba przeszukiwania: szybkie i pełne. Przeszukiwanie sieci Windows może nie wykryć urządzeń, na przykład, jeśli porty UDP 137, UDP 138, TCP 139 są zamknięte na routerze lub przez zaporę sieciową.

- **Przeszukiwanie Active Directory**. Serwer administracyjny pobiera informacje na temat struktury jednostki Active Directory i nazw DNS urządzeń z grup Active Directory. Domyślnie ten typ przeszukiwania jest włączony. Zalecane jest użycie przeszukiwania Active Directory, jeśli używasz Active directory; w przeciwnym razie Serwer administracyjny nie wykryje żadnych urządzeń. Jeśli używasz Active Directory, ale niektóre z urządzeń w sieci nie są wymienione jako członkowie, te urządzenia nie mogą być wykrywane przez przeszukiwanie Active Directory.

- **Przeszukiwanie zakresu IP**. Serwer administracyjny przeszukuje określone zakresy IP przy użyciu pakietów ICMP lub protokołu NBNS i sporządza pełen zestaw danych na temat urządzeń znajdujących się w tych zakresach IP. Domyślnie ten typ przeszukiwania jest wyłączony. Nie jest zalecane korzystanie z tego typu przeszukiwania, jeśli korzystasz z przeszukiwania sieci Windows i/lub przeszukiwania Active Directory.

- **Przeszukiwanie Zeroconf**. Punkt dystrybucji, który odpytuje sieć IPv6 za pomocą zero-configuration networking (zwany również *Zeroconf*). Domyślnie ten typ przeszukiwania jest wyłączony. Możesz użyć przeszukiwania Zeroconf, jeśli na punkcie dystrybucji działa system Linux.

Jeśli skonfigurowałeś i włączyłeś reguły przenoszenia urządzeń, nowo wykryte urządzenia są automatycznie umieszczane w grupie **Zarządzane urządzenia**. Jeśli nie włączono żadnych reguł przenoszenia, nowo wykryte urządzenia zostają automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**.

Możesz zmodyfikować ustawienia wykrywania urządzeń dla każdego typu. Na przykład, możesz chcieć zmodyfikować terminarz przeszukiwania lub ustawić, czy przeszukiwany ma być cały las Active Directory lub tylko określona domena.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB1 jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Użyj następującego polecenia:
`Get-SmbServerConfiguration | select EnableSMB1Protocol`

Przeszukiwanie sieci Windows

Informacje o przeszukiwaniu sieci Windows

Podczas szybkiego przeszukiwania Serwer administracyjny pobiera wyłącznie informacje o urządzeniach znajdujących się na liście nazw NetBIOS wszystkich domen sieci i grup roboczych. Podczas pełnego przeszukiwania wymagane są następujące informacje o każdym urządzeniu klienckim:

- Nazwa systemu operacyjnego
- Adres IP
- Nazwa DNS
- Nazwa NetBIOS

Szybkie przeszukiwanie i pełne przeszukiwanie wymagają:

- Porty UDP 137/138, TCP 139, UDP 445, TCP 445 muszą być dostępne w sieci.
- Protokół SMB jest włączony.
- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na Serwerze administracyjnym.
- Usługa Przeglądarka komputera Microsoft musi być używana, a główna przeglądarka komputera musi być włączona na urządzeniach klienckich:
  - Przynajmniej na jednym urządzeniu, jeśli liczba urządzeń w sieci nie przekracza 32.
  - Przynajmniej na jednym urządzeniu dla każdego z 32 urządzeń w sieci.

Pełne przeszukiwanie może być uruchomione tylko wtedy, gdy szybkie przeszukiwanie było uruchomione przynajmniej raz.

Przeglądanie i modyfikowanie ustawień przeszukiwania sieci Windows

W celu zmodyfikowania właściwości przeszukiwania sieci Windows:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Domeny Windows**.
2. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości domeny Windows.
3. Włącz lub wyłącz przeszukiwanie sieci Windows przy użyciu przycisku przełącznika **Włącz przeszukiwanie sieci Windows**.
4. Skonfiguruj terminarz przeszukiwania. Domyślnie, szybkie przeszukiwanie jest uruchamiane co 15 minut, a pełne przeszukiwanie jest uruchamiane co 60 minut.

   Dostępne są następujące opcje terminarza przeszukiwania:

   - **Co N dni**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

     Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.
   - **Co N minut**

     Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.
   - **Według dni tygodnia**

     Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.
   - **Co miesiąc, w określone dni wybranych tygodni**

Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

- Uruchom pominięte zadania

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest wyłączona.

5. Kliknij przycisk **Zapisz**.

Właściwości są zapisywane i stosowane do wszystkich wykrytych domen i podgrup systemu Windows.

Ręczne uruchamianie przeszukiwania

W celu natychmiastowego uruchomienia przeszukiwania:

Kliknij **Uruchom szybkie przeszukiwanie** lub **Uruchom pełne przeszukiwanie**.

Po zakończeniu przeszukiwania, możesz przejrzeć listę wykrytych urządzeń na stronie **Domeny Windows**, zaznaczając pole obok nazwy domeny, a następnie klikając przycisk **Urządzenia**.

Przeszukiwanie Active Directory

Użyj przeszukiwania Active Directory, jeśli używasz Active Directory; w innym przypadku zalecane jest użycie innych typów przeszukiwania. Jeśli używasz Active Directory, ale niektóre z urządzeń w sieci nie są wymienione jako członkowie, te urządzenia nie mogą być wykrywane przy użyciu przeszukiwania Active Directory.

Kaspersky Security Center wysyła żądanie do kontrolera domeny i otrzymuje strukturę urządzenia Active Directory. Przeszukiwanie Active Directory odbywa się co godzinę.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB1 jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Użyj następującego polecenia:
`Get-SmbServerConfiguration | select EnableSMB1Protocol`

Przeglądanie i modyfikowanie ustawień przeszukiwania Active Directory

W celu przejrzenia i zmodyfikowania ustawień przeszukiwania Active Directory:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Active Directory**.

2. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości Active Directory.

3. W oknie właściwości Active Directory możesz zdefiniować następujące ustawienia:

   a. Włącz lub wyłącz przeszukiwanie Active Directory, przy użyciu przycisku przełącznika.

   b. Zmień terminarz przeszukiwania.

      Domyślny przedział czasu wynosi jedną godzinę. Dane otrzymane przy kolejnym przeszukiwaniu całkowicie zastępują starsze dane.

   c. Skonfiguruj zaawansowane ustawienia, aby wybrać obszar przeszukiwania:

      - Domena Active Directory, do której należy Kaspersky Security Center
      - Las domeny, do którego należy Kaspersky Security Center
      - Określona lista domen Active Directory

      Aby dodać domenę do obszaru przeszukiwania, wybierz opcję domeny, kliknij przycisk **Dodaj**, a następnie określ adres kontrolera domeny oraz nazwę i hasło dla konta, aby uzyskać do niego dostęp.

4. W celu zastosowania nowych ustawień należy kliknąć przycisk **Zapisz**.

Nowe ustawienia zostaną zastosowane do przeszukiwania Active Directory.

Ręczne uruchamianie przeszukiwania

W celu natychmiastowego uruchomienia przeszukiwania:

Kliknij **Uruchom przeszukiwanie**.

Przeglądanie wyników przeszukiwania Active Directory

W celu przejrzenia wyników przeszukiwania Active Directory:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Active Directory**.

   Zostanie wyświetlona lista wykrytych jednostek organizacyjnych.

2. Jeśli chcesz, wybierz jednostkę organizacyjną, a następnie kliknij przycisk **Urządzenia**.

   Zostanie wyświetlona lista urządzeń w jednostce organizacyjnej.

Możesz przeszukać listę i filtrować wyniki.

Przeszukiwanie zakresu IP

Na początku program Kaspersky Security Center uzyskuje zakresy adresów IP dla przeszukiwania z ustawień sieciowych urządzenia, na którym jest zainstalowany. Jeśli adres urządzenia to 192.168.0.1, a maska podsieci to 255.255.255.0, Kaspersky Security Center uwzględnia sieć 192.168.0.0/24 na liście automatycznego przeszukiwania adresów. Kaspersky Security Center przeszukuje wszystkie adresy od 192.168.0.1 do 192.168.0.254.

Nie jest zalecane korzystanie z przeszukiwania zakresu IP, jeśli korzystasz z przeszukiwania sieci Windows i/lub przeszukiwania Active Directory.

Kaspersky Security Center może odpytywać zakresy adresów IP przez odwrotne wyszukiwanie DNS lub przy użyciu protokołu NBNS:

- **Odwrotne wyszukiwanie DNS**

  Kaspersky Security Center próbuje przeprowadzić odwrotne rozwiązanie nazwy dla każdego adresu IP z określonego zakresu do nazwy DNS przy użyciu standardowych żądań DNS. Jeśli to działanie zakończy się sukcesem, serwer wyśle `ICMP ECHO REQUEST` (to samo co polecenie ping) do otrzymanej nazwy. Jeśli urządzenie odpowie, informacje o tym zostaną dodane do bazy danych Kaspersky Security Center. Odwrotne rozwiązanie nazwy jest potrzebne do wykluczenia urządzeń sieciowych, które mogą mieć adres IP, ale nie komputery, na przykład, drukarki sieciowe lub routery.

  Ta metoda przeszukiwania polega na poprawnie skonfigurowanej lokalnej usłudze DNS. Musi mieć strefę wyszukiwania wstecznego. W sieciach, w których używane jest Active Directory, taka strefa jest obsługiwana automatycznie. Ale w tych sieciach przeszukiwanie podsieci IP nie zawiera więcej informacji niż przeszukiwanie Active Directory. Co więcej, administratorzy małych sieci często nie konfigurują strefy wyszukiwania wstecznego, ponieważ nie jest to konieczne dla pracy wielu usług sieciowych. Z tych powodów przeszukiwanie podsieci IP jest wyłączone domyślnie.

- **Protokół NBNS**

  Jeśli z jakiegoś powodu odwrotne rozpoznawanie nazw nie jest możliwe w Twojej sieci, Kaspersky Security Center używa protokołu NBNS do odpytywania zakresów IP. Jeśli żądanie skierowane do adresu IP zwróci nazwę NetBIOS, informacje o tym urządzeniu zostaną dodane do bazy danych Kaspersky Security Center.

Przed rozpoczęciem odpytywania sieci upewnij się, że protokół SMB1 jest włączony. W przeciwnym razie Kaspersky Security Center nie może wykryć urządzeń w odpytywanej sieci. Użyj następującego polecenia: `Get-SmbServerConfiguration | select EnableSMB1Protocol`

Przeglądanie i modyfikowanie ustawień przeszukiwania zakresu IP

W celu przejrzenia i zmodyfikowania właściwości przeszukiwania zakresu IP:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.

2. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno właściwości przeszukiwania IP.

3. Włącz lub wyłącz przeszukiwanie IP przy użyciu przycisku przełącznika **Zezwól na przeszukiwanie**.

4. Skonfiguruj terminarz przeszukiwania. Domyślnie, przeszukiwanie IP jest uruchamiane co 420 minut (siedem godzin).

   Podczas określania przedziału czasu przeszukiwania upewnij się, że to ustawienie nie przekracza wartości Parametr czasu dzierżawy adresu IP. Jeśli adres IP nie został zweryfikowany przez przeszukiwanie w trakcie czasu dzierżawy adresu IP, ten adres IP jest automatycznie usuwany z wyników przeszukiwania. Domyślnie, wyniki przeszukiwania są ważne 24 godziny, ponieważ dynamiczne adresy IP (przypisane przy użyciu Protokołu dynamicznej konfiguracji hosta (DHCP)) zmieniają się co 24 godziny.

   Dostępne są następujące opcje terminarza przeszukiwania:

- **Co N dni**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N minut**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

- **Według dni tygodnia**

  Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

- **Co miesiąc, w określone dni wybranych tygodni**

  Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest wyłączona.

5. Kliknij przycisk **Zapisz**.

Właściwości zostaną zapisane i zastosowane do wszystkich zakresów IP.

Ręczne uruchamianie przeszukiwania

W celu natychmiastowego uruchomienia przeszukiwania:

Kliknij **Uruchom przeszukiwanie**.

Dodawanie i modyfikowanie zakresu IP

Na początku program Kaspersky Security Center uzyskuje zakresy adresów IP dla przeszukiwania z ustawień sieciowych urządzenia, na którym jest zainstalowany. Jeśli adres urządzenia to 192.168.0.1, a maska podsieci to 255.255.255.0, Kaspersky Security Center uwzględnia sieć 192.168.0.0/24 na liście automatycznego przeszukiwania adresów. Kaspersky Security Center przeszukuje wszystkie adresy od 192.168.0.1 do 192.168.0.254. Możesz zmodyfikować automatycznie definiowany zakres adresów IP lub dodać niestandardowe zakresy adresów IP.

Możesz utworzyć zakres tylko dla adresów IPv4. Jeśli włączysz Przeszukiwanie Zeroconf, Kaspersky Security Center przeszuka całą sieć.

W celu dodania nowego zakresu IP:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.
2. Aby dodać nowy zakres IP, kliknij przycisk **Dodaj**.
3. W otwartym oknie określ następujące ustawienia:
   - **Nazwa zakresu IP**

     Nazwa zakresu IP. Możesz określić sam zakres IP jako nazwę, na przykład: „192.168.0.0/24”.
   - **Zakres IP lub adres podsieci i maska**

     Ustaw zakres IP, określając początkowy i końcowy adres IP lub adres podsieci i maskę podsieci. Możesz także wybrać jeden z już istniejących zakresów IP, klikając przycisk **Przeglądaj**.
   - **Okres istnienia adresu IP (godz.)**

     Podczas określania tego parametru upewnij się, że przekracza on czas przeszukiwania ustawiony w terminarzu przeszukiwania. Jeśli adres IP nie został zweryfikowany przez przeszukiwanie w trakcie czasu dzierżawy adresu IP, ten adres IP jest automatycznie usuwany z wyników przeszukiwania. Domyślnie, wyniki przeszukiwania są ważne 24 godziny, ponieważ dynamiczne adresy IP (przypisane przy użyciu Protokołu dynamicznej konfiguracji hosta - DHCP) zmieniają się co 24 godziny.
4. Wybierz **Włącz przeszukiwanie zakresu IP**, jeśli chcesz przeszukać podsieć lub przedział, które dodałeś. W przeciwnym razie, dodana podsieć lub przedział nie zostaną przeszukane.
5. Kliknij przycisk **Zapisz**.

Nowy zakres IP jest dodawany do listy zakresów IP.

Możesz uruchomić przeszukiwanie każdego zakresu IP oddzielnie, korzystając z przycisku **Uruchom przeszukiwanie**. Po zakończeniu przeszukiwania, możesz przejrzeć listę wykrytych urządzeń, korzystając z przycisku **Urządzenia**. Domyślnie, wyniki przeszukiwania są ważne 24 godziny, co jest równe ustawieniu czasu dzierżawy adresu IP.

W celu dodania podsieci do istniejącego zakresu IP:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.
2. Kliknij nazwę zakresu IP, do którego chcesz dodać podsieć.

3. W otwartym oknie kliknij przycisk **Dodaj**.

4. Określ podsieć, używając jej adresu i maski lub używając pierwszego i ostatniego adresu IP w zakresie IP. Lub dodaj istniejącą podsieć, klikając przycisk **Przeglądaj**.

5. Kliknij przycisk **Zapisz**.

   Nowa podsieć zostanie dodana do zakresu IP.

6. Kliknij przycisk **Zapisz**.

Zostaną zapisane nowe ustawienia zakresu IP.

Możesz dodać tyle podsieci, ile potrzebujesz. Nazwane zakresy IP nie mogą się nakładać, ale nienazwane podsieci wewnątrz zakresu IP nie posiadają takich ograniczeń. Możesz włączać i wyłączać przeszukiwanie niezależnie dla każdego zakresu IP.

Przeszukiwanie Zeroconf

Ten typ przeszukiwania jest obsługiwany tylko w przypadku punktów dystrybucji opartych na systemie Linux.

Punkt dystrybucji może przeszukiwać sieci, które mają urządzenia z adresami IPv6. W takim przypadku zakresy adresów IP nie są określone, a punkt dystrybucji przeszukuje całą sieć za pomocą zero-configuration networking (zwany również *Zeroconf*). Aby rozpocząć korzystanie z Zeroconf, musisz zainstalować narzędzie avahi-browse w punkcie dystrybucji.

W celu włączenia przeszukiwania sieci IPv6:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Zakresy IP**.

2. Kliknij przycisk **Właściwości**.

3. W otwartym oknie przełącz przycisk przełącznika **Użyj Zeroconf do przeszukiwania sieci IPv6**.

Następnie punkt dystrybucji zaczyna przeszukiwać sieć. W takim przypadku określone zakresy adresów IP są ignorowane.

Konfigurowanie reguły zatrzymania dla urządzeń nieprzypisanych

Po zakończeniu przeszukiwania sieci Windows, wykryte urządzenia zostały umieszczone w podgrupach grupy administracyjnej Urządzenia nieprzypisane. Tę grupę administracyjną można znaleźć w **Wykrywanie i wdrażanie** → **Wykrywanie** → **Domeny Windows**. Folder **Domeny Windows** to grupa nadrzędna. Zawiera grupy potomne, które zostały nazwane po odpowiednich domenach i grupach roboczych, które zostały wykryte podczas przeszukiwania. Grupa nadrzędna może także zawierać grupę administracyjną urządzeń mobilnych. Możesz skonfigurować reguły zatrzymania urządzeń nieprzypisanych dla grupy nadrzędnej i dla każdej grupy potomnej. Reguły zatrzymania nie zależą od ustawień wyszukiwania urządzeń i działają nawet wtedy, gdy wyszukiwanie urządzeń jest wyłączone.

W celu skonfigurowania reguł zatrzymania dla urządzeń nieprzypisanych:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Domeny Windows**.

2. Wykonaj jedną z poniższych czynności:

- Aby skonfigurować ustawienia grupy nadrzędnej, kliknij przycisk **Właściwości**.

  Zostanie otwarte okno właściwości domeny Windows.

- Aby skonfigurować ustawienia grupy potomnej, kliknij jej nazwę.

  Zostanie otwarte okno właściwości grupy potomnej.

3. Określ następujące ustawienia:

- **Usuń urządzenie z grupy, jeżeli było nieaktywne dłużej niż (dni)**

  Jeśli ta opcja jest włączona, możesz określić przedział czasu, po upływie którego urządzenie zostanie automatycznie usunięte z grupy. Domyślnie, ta opcja jest także rozsyłana do grup potomnych. Domyślny przedział czasu wynosi 7 dni.

  Domyślnie opcja ta jest włączona.

- **Dziedzicz z grupy nadrzędnej**

  Jeśli ta opcja jest włączona, okres zatrzymania dla urządzeń w bieżącej grupie jest dziedziczony z grupy nadrzędnej nie może zostać zmieniony.

  Ta opcja jest dostępna tylko dla grup potomnych.

  Domyślnie opcja ta jest włączona.

- **Wymuś dziedziczenie w grupach podrzędnych**

  Wartości ustawień zostaną rozesłane do grup potomnych, ale we właściwościach grup potomnych te ustawienia są zablokowane.

  Domyślnie opcja ta jest wyłączona.

4. Kliknij przycisk **Zaakceptuj**.

Twoje zmiany zostaną zapisane i zastosowane.

Aplikacje Kaspersky: licencjonowanie i aktywacja

Ta sekcja opisuje funkcje Kaspersky Security Center związane z pracą z kluczami licencyjnymi dla zarządzanych aplikacji Kaspersky.

Kaspersky Security Center pozwala na wykonywanie scentralizowanego rozsyłania kluczy licencyjnych dla aplikacji Kaspersky na urządzenia klienckie, monitorowanie ich wykorzystania i odnawianie licencji.

Dodając klucz licencyjny przy pomocy Kaspersky Security Center, jego ustawienia są zapisywane na Serwerze administracyjnym. W oparciu o te informacje, aplikacja generuje raport użycia klucza licencyjnego i powiadamia administratora o wygaśnięciu licencji oraz naruszeniu ograniczeń licencyjnych, określonych we właściwościach kluczy licencyjnych. Możesz skonfigurować powiadomienia związane z korzystaniem z kluczy licencyjnych w ustawieniach Serwera administracyjnego.

Licencjonowanie zarządzanych aplikacji

Aplikacje Kaspersky, zainstalowane na zarządzanych urządzeniach, muszą być licencjonowane poprzez zastosowanie pliku klucza lub kodu aktywacyjnego do każdej z aplikacji. Plik klucza lub kod aktywacyjny może zostać rozesłany w następujące sposoby:

- Automatyczne rozsyłanie
- Pakiet instalacyjny zarządzanej aplikacji
- Zadanie *Dodaj klucz licencyjny* dla zarządzanej aplikacji
- Ręczna aktywacja zarządzaną aplikacją

Możesz dodać nowy aktywny lub zapasowy klucz licencyjny za pomocą dowolnej z metod wymienionych powyżej. Aplikacja firmy Kaspersky używa w danej chwili aktywnego klucza i przechowuje zapasowy klucz do zastosowania po wygaśnięciu aktywnego klucza. Aplikacja, dla której dodajesz klucz licencyjny, określa, czy klucz jest aktywny, czy zapasowy. Definicja klucza nie zależy od metody użytej do dodania nowego klucza licencyjnego.

Automatyczne rozsyłanie

Jeśli używasz różnych zarządzanych aplikacji i musisz rozesłać określony plik klucza lub kod aktywacyjny na urządzenia, zdecyduj się na inne sposoby wdrożenia tego kodu aktywacyjnego lub pliku klucza.

Kaspersky Security Center umożliwia automatyczne rozesłanie dostępnych kluczy licencyjnych na urządzenia. Na przykład, trzy klucze licencyjne są przechowywane w repozytorium Serwera administracyjnego. Zaznaczyłeś pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** dla wszystkich trzech kluczy licencyjnych. Aplikacja zabezpieczająca Kaspersky—na przykład Kaspersky Endpoint Security for Windows—jest zainstalowana na urządzeniach w organizacji. Zostanie wykryte nowe urządzenie, do którego musi być rozesłany klucz licencyjny. Aplikacja określi, na przykład, że na urządzenie mogą zostać rozesłane dwa klucze licencyjne z repozytorium: klucz licencyjny o nazwie *Key_1* oraz klucz licencyjny o nazwie *Key_2*. Jeden z tych kluczy licencyjnych zostanie zastosowany na urządzeniu. W tym przypadku nie można przewidzieć, który z dwóch kluczy licencyjnych zostanie rozesłany na urządzenie, ponieważ automatyczne rozesłanie kluczy licencyjnych nie oferuje administratorowi podejmowania żadnych działań.

Podczas rozsyłania klucza licencyjnego urządzenia są zliczane dla tego klucza licencyjnego. Musisz upewnić się, że liczba urządzeń, na których klucz licencyjny został zastosowany, nie przekracza limitu określonego przez licencję. Jeśli liczba urządzeń przekracza limit określony przez licencję, wszystkie urządzenia, które nie zostały objęte licencją, otrzymają stan *Krytyczny*.

Przed zdalną instalacją, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Automatyczne rozsyłanie kluczy licencyjnych

  lub

- Kaspersky Security Center Web Console:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Automatyczne rozsyłanie kluczy licencyjnych

Dodawanie pliku klucza lub kodu aktywacyjnego do pakietu instalacyjnego zarządzanej aplikacji

Z powodów bezpieczeństwa, ta opcja nie jest zalecana. Plik klucza lub kod aktywacyjny dodane do pakietu instalacyjnego mogą być zagrożone.

Jeśli instalujesz zarządzaną aplikację przy użyciu pakietu instalacyjnego, możesz określić kod aktywacyjny lub plik klucza w tym pakiecie instalacyjnym lub w zasadzie aplikacji. Klucz licencyjny zostanie rozesłany na zarządzane urządzenia podczas kolejnej synchronizacji urządzenia z Serwerem administracyjnym.

Dostępne instrukcje:

- Konsola administracyjna:
  - Tworzenie pakietu instalacyjnego
  - Instalowanie aplikacji na urządzeniach klienckich

  lub
- Kaspersky Security Center Web Console: Dodawanie klucza licencyjnego do pakietu instalacyjnego

Rozesłanie poprzez zadanie Dodaj klucz licencyjny dla zarządzanej aplikacji

Jeśli zdecydujesz się na użycie zadania *Dodaj klucz licencyjny* dla zarządzanej aplikacji, możesz wybrać klucz licencyjny, który musi zostać rozesłany na urządzenia, oraz wybrać urządzenia w dowolny sposób—na przykład, wybierając grupę administracyjną lub wybór urządzeń.

Przed zdalną instalacją, plik klucza lub kod aktywacyjny musi zostać dodany do repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Rozsyłanie klucza licencyjnego na urządzenia klienckie

  lub
- Kaspersky Security Center Web Console:
  - Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego
  - Rozsyłanie klucza licencyjnego na urządzenia klienckie

Ręczne dodawanie kodu aktywacyjnego lub pliku klucza do urządzeń

Możesz aktywować zainstalowaną aplikację Kaspersky lokalnie, przy użyciu narzędzi dostępnych w interfejsie aplikacji. Więcej informacji można znaleźć w dokumentacji dla zainstalowanej aplikacji.

Dodawanie klucza licencyjnego do repozytorium Serwera administracyjnego

W celu dodania klucza licencyjnego do repozytorium Serwera administracyjnego:

1. W menu głównym przejdź do **Operacje** → **Licencjonowanie** → **Licencje Kaspersky**.
2. Kliknij przycisk **Dodaj**.
3. Wybierz, co chcesz dodać:
   - **Dodaj plik klucza**

     Kliknij przycisk **Wybierz plik klucza** i odszukaj plik .key, który chcesz dodać.
   - **Wprowadź kod aktywacyjny**

     Określ kod aktywacyjny w polu tekstowym i kliknij przycisk **Wyślij**.
4. Kliknij przycisk **Zamknij**.

Klucz licencyjny lub kilka kluczy licencyjnych zostaną dodane do repozytorium Serwera administracyjnego.

Rozsyłanie klucza licencyjnego na urządzenia klienckie

Kaspersky Security Center Web Console umożliwia rozesłanie klucza licencyjnego na urządzenia klienckie przy pomocy zadania *Rozsyłanie klucza licencyjnego*.

W celu rozesłania klucza licencyjnego na urządzenia klienckie:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. Wybierz aplikację, dla której chcesz dodać klucz licencyjny.
4. Z listy **Typ zadania** wybierz **Dodaj klucz licencyjny**.
5. Postępuj zgodnie z instrukcjami kreatora.
6. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
7. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

8. Aby uruchomić zadanie, na liście zadań wybierz zadanie i kliknij przycisk **Uruchom**.

Po wykonaniu zadania, klucz licencyjny zostanie rozesłany na wybrane urządzenia.

Automatyczne rozsyłanie kluczy licencyjnych

Kaspersky Security Center umożliwia automatyczne instalowanie kluczy licencyjnych na zarządzanych urządzeniach, jeśli znajdują się one w repozytorium kluczy licencyjnych na Serwerze administracyjnym.

W celu automatycznego rozsyłania kluczy licencyjnych do zarządzanych urządzeń:

1. W menu głównym przejdź do **Operacje → Licencjonowanie → Licencje Kaspersky**.
2. Kliknij nazwę klucza licencyjnego, który chcesz automatycznie rozesłać na urządzenia.
3. W otwartym oknie właściwości klucza licencyjnego zaznacz pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia**.
4. Kliknij przycisk **Zapisz**.

Klucz licencyjny zostanie automatycznie rozesłany do wszystkich kompatybilnych urządzeń.

Rozsyłanie klucza licencyjnego odbywa się przy pomocy Agenta sieciowego. Dla aplikacji nie są tworzone żadne zadania rozsyłania kluczy licencyjnych.

Podczas automatycznego rozsyłania klucza licencyjnego brane jest pod uwagę ograniczenie licencyjne dotyczące liczby urządzeń. Ograniczenie licencyjne jest ustawione we właściwościach klucza licencyjnego. Jeśli ograniczenie licencji zostanie osiągnięte, rozesłanie tego klucza licencyjnego na urządzenia zostanie przerwane automatycznie.

Jeśli zaznaczysz pole **Automatycznie roześlij klucz licencyjny na zarządzane urządzenia** w oknie właściwości klucza licencyjnego, klucz licencyjny jest natychmiast rozpowszechniany w Twojej sieci. Jeśli nie wybierzesz tej opcji, możesz ręcznie rozpowszechniać klucz licencyjny później.

Wyświetlanie informacji o używanych kluczach licencyjnych

W celu przejrzenia listy kluczy licencyjnych dodanych do repozytorium Serwera administracyjnego:

W menu głównym przejdź do **Operacje → Licencjonowanie → Licencje Kaspersky**.

Wyświetlona lista zawiera pliki klucza i kody aktywacyjne dodane do repozytorium Serwera administracyjnego.

W celu wyświetlenia szczegółowych informacji i kluczu licencyjnym:

1. W menu głównym przejdź do **Operacje → Licencjonowanie → Licencje Kaspersky**.
2. Kliknij nazwę żądanego klucza licencyjnego.

W otwartym oknie właściwości klucza licencyjnego możesz przejrzeć:

- Na zakładce **Ogólne**—główne informacje o kluczu licencyjnym
- Na zakładce **Urządzenia**—lista urządzeń klienckich, na których klucz licencyjny został użyty do aktywacji zainstalowanej aplikacji Kaspersky

W celu sprawdzenia, które klucze licencyjne zostały rozesłane na określone urządzenie klienckie:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.
2. Kliknij nazwę żądanego urządzenia.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Aplikacje**.
4. Kliknij nazwę aplikacji, dla której chcesz sprawdzić informacje o kluczu licencyjnym.
5. W otwartym oknie właściwości aplikacji wybierz zakładkę **Ogólne**, a następnie otwórz sekcję **Licencja**.

Zostaną wyświetlone główne informacje o aktywnych i zapasowych kluczach licencyjnych.

Aby określić aktualne ustawienia kluczy licencyjnych wirtualnego Serwera administracyjnego, Serwer administracyjny wysyła żądanie do serwerów aktywacji Kaspersky przynajmniej raz dziennie. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS.

Usuwanie klucza licencyjnego z repozytorium

Jeśli usuniesz aktywny klucz licencyjny dla dodatkowej funkcji Serwera administracyjnego, na przykład Zarządzanie lukami i poprawkami lub Zarządzanie urządzeniami mobilnymi, odpowiednia funkcja stanie się niedostępna. Jeśli dodano zapasowy klucz licencyjny, zapasowy klucz licencyjny automatycznie staje się aktywnym kluczem licencyjnym po wcześniejszym usunięciu aktywnego klucza licencyjnego.

Jeśli usuniesz aktywny klucz licencyjny rozesłany na zarządzane urządzenie, aplikacja będzie kontynuować pracę na zarządzanym urządzeniu.

W celu usunięcia pliku klucza lub kodu aktywacyjnego z repozytorium Serwera administracyjnego:

1. Sprawdź, czy Serwer administracyjny nie używa pliku klucza lub kodu aktywacyjnego, który chcesz usunąć. Jeśli tak, nie możesz usunąć klucza. Aby przeprowadzić kontrolę:
   a. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

      Zostanie otwarte okno właściwości Serwera administracyjnego.

   b. Na zakładce **Ogólne** wybierz sekcję **Klucze licencyjne**.
   c. Jeżeli w sekcji, która zostanie otwarta, pojawi się wymagany plik klucza lub kod aktywacyjny, kliknij przycisk **Usuń aktywny klucz licencyjny**, a następnie potwierdź operację. Następnie Serwer administracyjny nie używa usuniętego klucza licencyjnego, ale klucz pozostaje w repozytorium Serwera administracyjnego. Jeśli wymagany plik klucza lub kod aktywacyjny nie jest wyświetlany, serwer administracyjny go nie używa.
2. W menu głównym przejdź do **Operacje** → **Licencjonowanie** → **Licencje Kaspersky**.
3. Wybierz wymagany plik klucza lub kod aktywacyjny, a następnie kliknij przycisk **Usuń**.

Wybrany plik klucza lub kod aktywacyjny zostanie usunięty z repozytorium.

Możesz ponownie dodać usunięty klucz licencyjny lub dodać nowy klucz licencyjny.

Wycofanie zgody z Umową Licencyjną Użytkownika Końcowego

Jeśli zdecydujesz się na zatrzymanie ochrony niektórych swoich urządzeń klienckich, możesz wycofać zgodę z Umową licencyjną dla każdej zarządzanej aplikacji firmy Kaspersky. Przed wycofaniem zgody z Umową licencyjną należy odinstalować wybraną aplikację.

Umowy licencyjne, które zostały zaakceptowane na wirtualnym Serwerze administracyjnym, mogą zostać odrzucone na wirtualnym Serwerze administracyjnym lub na głównym Serwerze administracyjnym. Umowy licencyjne, które zostały zaakceptowane na głównym Serwerze administracyjnym, mogą zostać odrzucone tylko na głównym Serwerze administracyjnym.

W celu anulowania Umowy licencyjnej dla zarządzanych aplikacji Kaspersky:

1. Otwórz okno właściwości Serwera administracyjnego i na zakładce **Ogólne** wybierz sekcję **Umowy licencyjne użytkownika końcowego**.

   Wyświetlana jest lista Umów licencyjnych, zaakceptowanych po utworzeniu pakietów instalacyjnych, w momencie bezproblemowej instalacji aktualizacji lub po zdalnym zainstalowaniu Kaspersky Security for Mobile.

2. Z listy wybierz Umowę licencyjną, którą chcesz anulować.

   Możesz sprawdzić następujące właściwości Umowy licencyjnej:

   - Datę zaakceptowania Umowy licencyjnej
   - Nazwę użytkownika, który zaakceptował Umowę licencyjną

3. Kliknij datę zaakceptowania dowolnej Umowy licencyjnej, aby otworzyć jej okno właściwości wyświetlające następujące dane:

   - Nazwę użytkownika, który zaakceptował Umowę licencyjną
   - Datę zaakceptowania Umowy licencyjnej
   - Unikatowy identyfikator (UID) Umowy licencyjnej
   - Pełną treść Umowy licencyjnej
   - Listę obiektów (pakiety instalacyjne, aktualizacje typu seamless, aplikacje mobilne) powiązanych z Umową licencyjną oraz ich odpowiednie nazwy i typy

4. W lewej części okna właściwości Umowy licencyjnej kliknij przycisk **Odrzuć Umowę licencyjną**.

   Jeśli istnieją jakiekolwiek obiekty (pakiety instalacyjne i ich odpowiednie zadania), które uniemożliwiają wycofanie Umowy licencyjnej, zostanie wyświetlone odpowiednie powiadomienie. Jeśli nie usunąłeś tych obiektów, nie możesz przejść do wycofania.

   W otwartym oknie zostanie wyświetlona informacja, że w pierwszej kolejności musisz odinstalować aplikację firmy Kaspersky odpowiadającą Umowie licencyjnej.

5. Kliknij przycisk, aby potwierdzić wycofanie.

   Umowa licencyjna zostanie wycofana. Nie jest już wyświetlana na liście Umów licencyjnych w sekcji **Umowy licencyjne użytkownika końcowego**. Okno właściwości Umowy licencyjnej zostanie zamknięte; aplikacja nie będzie już zainstalowana.

Odnawianie licencji dla aplikacji Kaspersky

Możesz odnowić licencję dla aplikacji Kaspersky, która utraciła ważność lub wkrótce utraci ważność (za mniej niż 30 dni).

W celu odnowienia licencji, która utraciła ważność, lub licencji, która wkrótce utraci ważność:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź do **Operacje → Licencjonowanie → Licencje Kaspersky**.
   - W oknie głównym przejdź do **Monitorowanie i raportowanie → Pulpit nawigacyjny**, a następnie kliknij odnośnik **Zobacz wygasające licencje** obok powiadomienia.

   Zostanie otwarte okno **Licencje Kaspersky**, w którym możesz przejrzeć i odnowić licencje.

2. Kliknij łącze **Odnów licencję** obok wymaganej licencji.

   Klikając odnośnik do odnowienia licencji, wyrażasz zgodę na przeniesienie do Kaspersky następujących informacji o programie Kaspersky Security Center: jego wersję, wersję językową, której używasz, identyfikator licencji oprogramowania (czyli identyfikator odnawianej licencji), a także, czy zakupiłeś licencję u partnera firmy.

3. W otwartym oknie usługi odnowienia licencji wykonaj instrukcje w celu odnowienia licencji.

   Licencja zostanie odnowiona.

W Kaspersky Security Center Web Console powiadomienia o licencji, która wkrótce utraci ważność, są wyświetlane zgodnie z następującym terminarzem:

- 30 dni przed utratą ważności
- 7 dni przed utratą ważności
- 3 dni przed utratą ważności
- 24 godziny przed utratą ważności
- Po wygaśnięciu licencji

Korzystanie z Kaspersky Marketplace do wyboru rozwiązań biznesowych firmy Kaspersky

Platforma handlowa to sekcja w menu głównym, która umożliwia przeglądanie całej gamy rozwiązań biznesowych firmy Kaspersky, wybranie tych, których potrzebujesz, i przejście do zakupu na stronie internetowej Kaspersky. Możesz użyć filtrów, aby wyświetlić tylko te rozwiązania, które pasują do Twojej organizacji i wymagań systemu bezpieczeństwa informacji. Po wybraniu rozwiązania Kaspersky Security Center przekieruje Cię do powiązanej strony internetowej w witrynie Kaspersky, aby dowiedzieć się więcej o tym rozwiązaniu. Każda strona internetowa umożliwia przejście do zakupu lub zawiera instrukcje dotyczące procesu zakupu.

W sekcji **Platforma handlowa** możesz filtrować rozwiązania firmy Kaspersky z użyciem następujących kryteriów:

- Liczba urządzeń (punktów końcowych, serwerów i innych typów zasobów), które chcesz chronić:
  - 50–250
  - 250–1000
  - Więcej niż 1000
- Poziom dojrzałości zespołu ds. bezpieczeństwa informacji w Twojej organizacji:
  - **Podstawowy**

    Ten poziom jest typowy dla przedsiębiorstw, które posiadają tylko zespół ds. IT. Maksymalna możliwa liczba zagrożeń jest blokowana automatycznie.
  - **Optymalny**

    Ten poziom jest typowy dla przedsiębiorstw, które posiadają określoną funkcję bezpieczeństwa IT w zespole ds. IT. Na tym poziomie firmy potrzebują rozwiązań, które umożliwią im przeciwdziałanie zagrożeniom towarowym oraz zagrożeniom omijającym istniejące mechanizmy prewencyjne.
  - **Ekspert**

    Ten poziom jest typowy dla przedsiębiorstw o złożonych i rozproszonych środowiskach IT. Zespół ds. bezpieczeństwa IT jest dojrzały lub firma posiada zespół SOC (Security Operations Center). Wymagane rozwiązania umożliwiają firmom przeciwdziałanie złożonym zagrożeniom i atakom ukierunkowanym.
- Typy zasobów, które chcesz chronić:
  - **Punkty końcowe**: stacje robocze pracowników, maszyny fizyczne i wirtualne, systemy wbudowane
  - **Serwery**: serwery fizyczne i wirtualne
  - **Chmura**: środowiska chmury publicznej, prywatnej lub hybrydowej; usługi w chmurze
  - **Sieć**: sieć lokalna, infrastruktura IT
  - **Usługa**: usługi związane z bezpieczeństwem świadczone przez Kaspersky

W celu znalezienia i zakupu rozwiązania biznesowego firmy Kaspersky:

1. W oknie głównym przejdź do **Platforma handlowa**.

   Domyślnie sekcja wyświetla wszystkie dostępne rozwiązania biznesowe firmy Kaspersky.
2. Aby wyświetlić tylko te rozwiązania, które odpowiadają Twojej organizacji, wybierz wymagane wartości w filtrach.
3. Kliknij rozwiązanie, które chcesz kupić lub chcesz dowiedzieć się więcej.

Zostaniesz przekierowany na stronę rozwiązania. Możesz postępować zgodnie z instrukcjami wyświetlanymi na ekranie, aby przejść do zakupu.

Konfigurowanie ochrony sieci

Ta sekcja zawiera informacje o ręcznej konfiguracji zasad i zadań, informacje o rolach użytkownika, informacje o tworzeniu struktury grupy administracyjnej oraz hierarchii zadań.

Scenariusz: Konfigurowanie ochrony sieci

Kreator wstępnej konfiguracji tworzy zasady i zadania z domyślnymi ustawieniami. Te ustawienia mogą okazać się nieoptymalne lub nawet niedopuszczalne przez organizację. Dlatego zalecane jest dostrojenie tych profili i zadań oraz utworzenie innych profili i zadań, jeśli są konieczne w Twojej sieci.

Wymagania wstępne

Przed rozpoczęciem upewnij się, że:

- Zainstalowano Serwer administracyjny Kaspersky Security Center
- Zainstalowano Kaspersky Security Center Web Console (opcjonalne)
- Zakończyłeś główny scenariusz instalacji Kaspersky Security Center
- Zakończono działanie kreatora wstępnej konfiguracji lub ręcznie utworzono następujące zasady i zadania w grupie administracyjnej **Zarządzane urządzenia**:
  - Profil Kaspersky Endpoint Security
  - Grupowe zadanie aktualizacji Kaspersky Endpoint Security
  - Profil Agenta sieciowego
  - Zadanie *Wyszukiwania luk i wymaganych aktualizacji*

Konfigurowanie ochrony sieci odbywa się w etapach:

1. **Konfiguracja i przesyłanie profili i profili zasad aplikacji firmy Kaspersky**

   Aby skonfigurować i przesłać ustawienia dla aplikacji Kaspersky, zainstalowanych na zarządzanych urządzeniach, możesz użyć dwóch różnych metod zarządzania ochroną—skoncentrowaną na urządzeniu lub skoncentrowaną na użytkowniku. Te dwie metody można także połączyć. Aby zaimplementować zarządzanie ochroną skoncentrowaną na urządzeniu, możesz użyć narzędzi dostarczonych w Konsoli administracyjnej opartej na Microsoft Management Console lub Kaspersky Security Center Web Console. Zarządzanie ochroną skoncentrowaną na użytkowniku może zostać zaimplementowane tylko poprzez Kaspersky Security Center Web Console.

2. **Konfigurowanie zadań zdalnego zarządzania aplikacjami firmy Kaspersky**

   Sprawdź zadania utworzone przy pomocy kreatora wstępnej konfiguracji i dostosuj je (jeśli to konieczne).

Dostępne instrukcje:

- Konsola administracyjna:
  - Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security
  - Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
- Kaspersky Security Center Web Console:
  - Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security
  - Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

Jeśli to konieczne, utwórz dodatkowe zadania do zarządzania aplikacjami firmy Kaspersky, zainstalowanymi na urządzeniach klienckich.

3. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Dostępne instrukcje:

   - Konsola administracyjna: Konfigurowanie maksymalnej liczby zdarzeń
   - Kaspersky Security Center Web Console: Konfigurowanie maksymalnej liczby zdarzeń

Wyniki

Po zakończeniu tego scenariusza, Twoja sieć będzie chroniona przez konfigurację aplikacji Kaspersky, zadania i zdarzenia otrzymane przez Serwer administracyjny:

- Aplikacje firmy Kaspersky są konfigurowane zgodnie z zasadami i profilami zasad.
- Aplikacje są zarządzane za pośrednictwem zestawu zadań.
- Maksymalna liczba zdarzeń, jaka może być przechowywana w bazie danych, została ustawiona.

Jeśli konfiguracja ochrony sieci zostanie zakończona, możesz przejść do konfigurowania regularnych aktualizacji baz danych i aplikacji Kaspersky.

Więcej informacji o sposobie konfiguracji automatycznych odpowiedzi na zagrożenia wykryte przez Kaspersky Sandbox można znaleźć w pomocy online Kaspersky Sandbox 2.0.

Informacje o metodach zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku

Możesz zarządzać ustawieniami zabezpieczeń z poziomu funkcji urządzenia i z poziomu roli użytkownika. Pierwsza metoda nosi nazwę *zarządzanie ochroną skoncentrowaną na urządzeniu*, a druga nazywa się *zarządzania ochroną skoncentrowaną na użytkowniku*. Aby zastosować różne ustawienia aplikacji na różnych urządzeniach, możesz użyć połączonych typów zarządzania. Aby zaimplementować zarządzanie ochroną skoncentrowaną na urządzeniu, możesz użyć narzędzi dostarczonych w Konsoli administracyjnej opartej na Microsoft Management Console lub Kaspersky Security Center Web Console. Zarządzanie ochroną skoncentrowaną na użytkowniku może zostać zaimplementowane tylko poprzez Kaspersky Security Center Web Console.

Zarządzanie bezpieczeństwem skoncentrowane na urządzeniu umożliwia zastosowanie różnych ustawień bezpieczeństwa aplikacji na zarządzanych urządzeniach w zależności od funkcji charakterystycznych dla urządzeń. Na przykład, możesz zastosować różne ustawienia do urządzeń przydzielonych w różnych grupach administracyjnych. Możesz także rozróżnić urządzenia przy użyciu tych urządzeń w Active Directory lub ich specyfikacji sprzętowej.

Zarządzanie bezpieczeństwem skoncentrowanym na użytkowniku umożliwia zastosowanie różnych ustawień aplikacji zabezpieczającej do różnych ról użytkownika. Możesz utworzyć kilka ról użytkownika, przypisać odpowiednią rolę użytkownika do każdego użytkownika oraz określić różne ustawienia aplikacji do urządzeń należących do użytkowników z różnymi rolami. Na przykład, chcesz zastosować różne ustawienia aplikacji na urządzeniach księgowych i specjalistów z działu HR. W rezultacie, gdy zaimplementowane jest zarządzanie ochroną skoncentrowaną na użytkowniku, każdy dział—dział księgowych i dział HR—posiada swoją własną konfigurację ustawień dla aplikacji firmy Kaspersky. Konfiguracja ustawień definiuje, które ustawienia aplikacji mogą być zmieniane przez użytkowników i dla których wymuszone jest ustawienie i zablokowanie przez administratora.

Korzystając z zarządzania ochroną skoncentrowaną na użytkowniku, możesz zastosować określone ustawienia aplikacji do pojedynczych użytkowników. Może to być wymagane, gdy pracownik posiada unikatową rolę w firmie lub gdy chcesz monitorować incydenty bezpieczeństwa dotyczące urządzeń określonej osoby. W zależności od roli tego pracownika w firmie, możesz rozszerzyć lub ograniczyć uprawnienia tej osoby do zmiany ustawień aplikacji. Na przykład, możesz rozszerzyć uprawnienia administratora systemu, który zarządza urządzeniami klienckimi w biurze lokalnym.

Możesz połączyć metody zarządzania ochroną skoncentrowaną na urządzeniu i użytkowniku. Na przykład, możesz skonfigurować określony profil aplikacji dla każdej grupy administracyjnej, a następnie utworzyć profile zasad dla jednej lub kilku ról użytkownika Twojej firmy. W tym przypadku profile i profile zasad są stosowane w następującej kolejności:

1. Zostaną zastosowane profile utworzone dla zarządzania ochroną skoncentrowaną na urządzeniu.
2. Są one modyfikowane przez profile zasad zgodnie z priorytetami profili zasad.
3. Profile są modyfikowane przez profile zasad skojarzone z rolami użytkownika.

Konfiguracja i przydzielanie profili: Metoda skoncentrowana na urządzeniu

Po zakończeniu tego scenariusza, aplikacje zostaną skonfigurowane na wszystkich zarządzanych urządzeniach zgodnie z profilami i profilami zasad aplikacji, które określiłeś.

Wymagania wstępne

Przed rozpoczęciem konfiguracji upewnij się, że zainstalowano Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center Web Console (opcjonalnie). Jeśli zainstalowano Kaspersky Security Center Web Console, możesz wziąć pod uwagę zarządzania ochroną skoncentrowaną na użytkowniku jako alternatywę lub dodatkową opcję dla metody skoncentrowanej na urządzeniu.

Etapy

Scenariusz skoncentrowanego na urządzeniu zarządzania aplikacjami Kaspersky obejmuje następujące kroki:

1. **Konfigurowanie profili aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie profilu dla każdej aplikacji. Zestaw profili zostanie przesłany na urządzenia klienckie.

   Podczas konfigurowania ochrony sieci w kreatorze szybkiego startu Kaspersky Security Center tworzy domyślną politykę dla następujących aplikacji:

   - Kaspersky Endpoint Security for Windows — dla urządzeń klienckich z systemem Windows
   - Kaspersky Endpoint Security for Linux — dla urządzeń klienckich z Linux

   Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowego profilu dla tej aplikacji. Przejdź do ręcznej konfiguracji profilu Kaspersky Endpoint Security.

   Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i potomne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy potomne i podrzędne Serwery administracyjne, aby zabronić wszelkich modyfikacji ustawień skonfigurowanych w nadrzędnej zasadzie. Jeśli chcesz, żeby wymuszone było dziedziczenie tylko części ustawień, możesz zablokować je w profilu nadrzędnym. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w profilach podrzędnych. Utworzona hierarchia profili umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie profilu
   - Kaspersky Security Center Web Console: Tworzenie profilu

2. **Tworzenie profili zasad (opcjonalnie)**

   Jeśli chcesz, żeby urządzenia w jednej grupie administracyjnej były uruchamiane z różnymi ustawieniami profilu, utwórz profile zasad dla tych urządzeń. Profil zasad jest to inaczej podzbiór ustawień profilu. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z profilem i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od „podstawowego" profilu, który jest aktywny na zarządzanym urządzeniu.

   Korzystając z warunków aktywacji profilu, możesz zastosować różne profile zasad, na przykład, do urządzeń znajdujących się w określonej jednostce lub grupie bezpieczeństwa Active Directory, posiadającej określoną konfigurację sprzętową lub oznaczoną określonymi znacznikami. Użyj znaczników do filtrowania urządzeń, które spełniają określone kryteria. Na przykład, możesz utworzyć znacznik nazwany *Windows*, oznaczyć tym znacznikiem wszystkie urządzenia działające pod kontrolą systemu operacyjnego Windows, a następnie określić ten znacznik jako warunek aktywacji profilu zasad. W wyniku tego działania, aplikacje Kaspersky zainstalowane na wszystkich urządzeniach działających pod kontrolą systemu Windows będą zarządzane przez swój własny profil zasad.

   Dostępne instrukcje:

   - Konsola administracyjna:
     - Tworzenie profilu zasad
     - Tworzenie reguły aktywacji profilu zasad
   - Kaspersky Security Center Web Console:
     - Tworzenie profilu zasad

- Tworzenie reguły aktywacji profilu zasad

3. **Przesyłanie profili i profili zasad na zarządzane urządzenia**

   Domyślnie Serwer administracyjny automatycznie synchronizuje się z zarządzanymi urządzeniami co 15 minut. Możesz obejść automatyczną synchronizację i ręcznie uruchomić synchronizację przy pomocy polecenia Wymuś synchronizację. Synchronizacja jest również wymuszana po utworzeniu lub zmianie zasady lub profilu zasady. Podczas synchronizacji nowe lub zmienione profile i profile zasad zostają rozesłane na zarządzane urządzenia.

   Jeśli używasz Kaspersky Security Center Web Console, możesz sprawdzić, czy zasady i profile zasad zostały dostarczone na urządzenie. Kaspersky Security Center określa datę i godzinę dostarczenia we właściwościach urządzenia.

   Dostępne instrukcje:

   - Konsola administracyjna: Wymuszona synchronizacja
   - Kaspersky Security Center Web Console: Wymuszona synchronizacja

Wyniki

Po zakończeniu scenariusza skoncentrowanego na urządzeniu, aplikacje Kaspersky są konfigurowane zgodnie z ustawieniami określonymi i przesłanymi poprzez hierarchię profili.

Skonfigurowane profile i profile zasad aplikacji zostaną automatycznie zastosowane do nowych urządzeń dodanych do grup administracyjnych.

Konfiguracja i przydzielanie profili: Metoda skoncentrowana na użytkowniku

Ta sekcja opisuje scenariusz skoncentrowanej na użytkowniku scentralizowanej konfiguracji aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach. Po zakończeniu tego scenariusza, aplikacje zostaną skonfigurowane na wszystkich zarządzanych urządzeniach zgodnie z profilami i profilami zasad aplikacji, które określiłeś.

Ten scenariusz można zaimplementować za pomocą Kaspersky Security Center Web Console w wersji 13 lub nowszej.

Wymagania wstępne

Przed rozpoczęciem konfiguracji upewnij się, że pomyślnie zainstalowano Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center Web Console, a także zakończono główny scenariusz instalacji. Możesz wziąć pod uwagę zarządzanie ochroną skoncentrowaną na urządzeniu jako alternatywę lub dodatkową opcję dla metody skoncentrowanej na użytkowniku. Dowiedz się więcej na temat dwóch metod zarządzania.

Proces

Scenariusz skoncentrowanego na użytkowniku zarządzania aplikacjami Kaspersky obejmuje następujące kroki:

1. **Konfigurowanie profili aplikacji**

   Skonfiguruj ustawienia dla aplikacji firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach poprzez utworzenie profilu dla każdej aplikacji. Zestaw profili zostanie przesłany na urządzenia klienckie.

Jeśli konfigurujesz ochronę swojej sieci w kreatorze wstępnej konfiguracji, Kaspersky Security Center tworzy domyślny profil dla Kaspersky Endpoint Security. Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowego profilu dla tej aplikacji. Przejdź do ręcznej konfiguracji profilu Kaspersky Endpoint Security.

Jeśli masz hierarchiczną strukturę kilku Serwerów administracyjnych i/lub grup administracyjnych, domyślnie podrzędne Serwery administracyjne i potomne grupy administracyjne dziedziczą zasady z głównego Serwera administracyjnego. Możesz wymusić dziedziczenie przez grupy potomne i podrzędne Serwery administracyjne, aby zabronić wszelkich modyfikacji ustawień skonfigurowanych w nadrzędnej zasadzie. Jeśli chcesz, żeby wymuszone było dziedziczenie tylko części ustawień, możesz zablokować je w profilu nadrzędnym. Pozostałe niezablokowane ustawienia będą dostępne do modyfikacji w profilach podrzędnych. Utworzona hierarchia profili umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

Dostępne instrukcje: Tworzenie profilu

2. **Określanie właścicieli urządzeń**

   Przypisz zarządzane urządzenia do odpowiednich użytkowników.

   Dostępne instrukcje: Wskazywanie użytkownika jako właściciela urządzenia

3. **Określanie ról użytkownika typowych dla Twojej firmy**

   Pomyśl o różnych rodzajach pracy, jaką pracownicy Twojej firmy zazwyczaj wykonują. Musisz podzielić wszystkich pracowników zgodnie z ich rolami. Na przykład, możesz podzielić ich według działów, profesji lub pozycji. Następnie musisz utworzyć rolę użytkownika dla każdej grupy. Pamiętaj, że każda rola użytkownika będzie posiadała swój własny profil zasad zawierający ustawienia aplikacji specyficzne dla tej roli.

4. **Tworzenie ról użytkownika**

   Utwórz i skonfiguruj rolę użytkownika dla każdej grupy pracowników, którą określiłeś w poprzednim kroku, lub użyj predefiniowanej roli użytkownika. Role użytkownika będą zawierały zestaw uprawnień dostępu do funkcji aplikacji.

   Dostępne instrukcje: Tworzenie roli użytkownika

5. **Określanie obszaru każdej roli użytkownika**

   Dla każdej utworzone roli użytkownika określ użytkowników i/lub grupy bezpieczeństwa oraz grupy administracyjne. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup potomnych.

   Dostępne instrukcje: Edytowanie obszaru roli użytkownika

6. **Tworzenie profili zasad**

   Utwórz profil zasad dla każdej roli użytkownika w Twojej firmie. Profile zasad określają, które ustawienia zostaną zastosowane w aplikacjach zainstalowanych na urządzeniach użytkowników w zależności od roli każdego użytkownika.

   Dostępne instrukcje: Tworzenie profilu zasad

7. **Kojarzenie profili zasad z rolami użytkownika**

   Skojarz utworzone profile zasad z rolami użytkownika. Następnie: profil zasad stanie się aktywny dla użytkowników, którzy posiadają określoną rolę. Ustawienia skonfigurowane w profilu zasad zostaną zastosowane do aplikacji Kaspersky zainstalowanych na urządzeniach użytkownika.

   Dostępne instrukcje: Kojarzenie profili zasad z rolami

8. **Przesyłanie profili i profili zasad na zarządzane urządzenia**

Domyślnie Serwer administracyjny automatycznie synchronizuje się z zarządzanymi urządzeniami co 15 minut. Podczas synchronizacji nowe lub zmienione profile i profile zasad zostają rozesłane na zarządzane urządzenia. Możesz obejść automatyczną synchronizację i ręcznie uruchomić synchronizację przy pomocy polecenia Wymuś synchronizację. Po zakończeniu synchronizacji, aby zapewnić dostarczenie i zastosowanie profili i profili zasad do zainstalowanych aplikacji Kaspersky.

Możesz sprawdzić, czy profile i profile zasad zostały dostarczone na urządzenie. Kaspersky Security Center określa datę i godzinę dostarczenia we właściwościach urządzenia.

Dostępne instrukcje: Wymuszona synchronizacja

Wyniki

Po zakończeniu scenariusza skoncentrowanego na użytkowniku, aplikacje Kaspersky są konfigurowane zgodnie z określonymi ustawieniami i przesyłane poprzez hierarchię profili i profili zasad.

Dla nowego użytkownika konieczne będzie utworzenie nowego konta, przypisanie użytkownikowi jednej z utworzonych ról użytkownika, a także przypisane urządzeń do użytkownika. Skonfigurowane profile i profile zasad aplikacji zostaną automatycznie zastosowane do urządzeń tego użytkownika.

Ustawienia zasady Agenta sieciowego

W celu skonfigurowania zasady Agenta sieciowego:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij nazwę zasady Agenta sieciowego.
   Zostanie otwarte okno właściwości zasady Agenta sieciowego.

Weź pod uwagę, że dla urządzeń z systemami Windows, macOS i Linux dostępne są różne ustawienia.

Ogólne

Na tej zakładce możesz zmodyfikować stan zasady oraz określić dziedziczenie ustawień zasady:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:
  - **Aktywny**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.

  - **Nieaktywny**

    Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.

- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:
  - **Dziedzicz ustawienia z zasady nadrzędnej**

Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

Domyślnie opcja ta jest włączona.

- Wymuś dziedziczenie ustawień w zasadach podrzędnych

  Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:

  - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.
  - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

  Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

  Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Na tej zakładce możesz skonfigurować rejestrowania zdarzeń oraz powiadamianie o zdarzeniach. Zdarzenia są rozsyłane zgodnie z priorytetem w następujących sekcjach na zakładce **Konfiguracja zdarzenia**:

- **Błąd funkcjonalny**
- **Ostrzeżenie**
- **Informacja**

W każdej sekcji, lista typów zdarzeń wyświetla typy zdarzeń oraz domyślny czas przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Po kliknięciu typu zdarzenia możesz określić ustawienia zapisywania zdarzeń oraz powiadomień o zdarzeniach wybranych z listy. Domyślnie, podstawowe ustawienia powiadamiania, określone dla całego Serwera administracyjnego, są używane dla wszystkich typów zdarzeń. Jednakże możesz zmienić określone ustawienia dla żądanych typów zdarzeń.

Na przykład, w sekcji **Ostrzeżenie** możesz skonfigurować typ zdarzenia **Wystąpił incydent**. Takie zdarzenia mogą mieć miejsce, na przykład, gdy wolne miejsce na dysku punktu dystrybucji jest mniejsze niż 2 GB (co najmniej 4 GB są wymagane do zdalnego instalowania aplikacji i pobierania aktualizacji). Aby skonfigurować zdarzenie **Wystąpił incydent**, kliknij je i określ, gdzie mają być przechowywane zdarzenia i jak powiadamiać o nich.

Jeśli Agent sieciowy wykrył incydent, możesz nim zarządzać za pomocą ustawień zarządzanego urządzenia.

Ustawienia aplikacji

Ustawienia

W sekcji **Ustawienia** możesz skonfigurować zasadę Agenta sieciowego:

- Rozsyłaj pliki tylko poprzez punkty dystrybucji

Jeśli ta opcja jest włączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia tylko z punktów dystrybucji.

Jeśli ta opcja jest wyłączona, Agenty sieciowe na zarządzanych urządzeniach pobierają uaktualnienia z punktów dystrybucji lub z Serwera administracyjnego.

Należy pamiętać, że aplikacje zabezpieczające na zarządzanych urządzeniach pobierają uaktualnienia ze źródła ustawionego w zadaniu aktualizacji dla każdej aplikacji zabezpieczającej. Jeśli włączysz opcję **Rozsyłaj pliki tylko poprzez punkty dystrybucji**, upewnij się, że Kaspersky Security Center jest ustawiony jako źródło uaktualnień w zadaniach aktualizacji.

Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar kolejki zdarzeń, w MB**

  W tym polu możesz określić maksymalny rozmiar przestrzeni dyskowej zajmowanej przez kolejkę zdarzenia.

  Domyślna wartość to 2 megabajty (MB).

- **Aplikacja może pobierać rozszerzone dane zasad na urządzenie**

  Agent sieciowy zainstalowany na zarządzanym urządzeniu przesyła informacje o zastosowanej zasadzie aplikacji zabezpieczającej (na przykład, Kaspersky Endpoint Security for Windows). Przesłane informacje możesz przejrzeć w interfejsie aplikacji zabezpieczającej.

  Agent sieciowy przesyła następujące informacje:

  - Czas dostarczenia zasady na zarządzane urządzenie
  - Nazwę aktywnej zasady lub zasady użytkownika mobilnego w momencie dostarczenia zasady na zarządzane urządzenie
  - Nazwę i pełną ścieżkę do grupy administracyjnej, która zawierała zarządzane urządzenie w momencie dostarczenia zasady na zarządzane urządzenie
  - Lista aktywnych profili zasad

    Możesz użyć informacji, aby zapewnić, że poprawna zasada zostanie zastosowana do urządzenia oraz aby rozwiązać problemy. Domyślnie opcja ta jest wyłączona.

- **Chroń usługę Agenta sieciowego przed nieuprawnionym usuwaniem, zatrzymywaniem i zmianami ustawień**

  Po zainstalowaniu Agenta sieciowego na zarządzanym urządzeniu, komponent nie może zostać usunięty ani ponownie skonfigurowany bez żądanych uprawnień. Usługa Agenta sieciowego nie może zostać zatrzymana.

  Domyślnie opcja ta jest wyłączona.

- **Użyj hasła dezinstalacyjnego**

  Jeśli ta opcja jest włączona, klikając przycisk **Modyfikuj**, można określić hasło do zdalnej dezinstalacji Agenta sieciowego.

  Domyślnie opcja ta jest wyłączona.

Repozytoria

W sekcji **Repozytoria** możesz wybrać typy obiektów, których szczegóły zostaną wysłane z Agenta sieciowego na Serwer administracyjny. Jeśli modyfikacja niektórych ustawień w tej sekcji jest zablokowana przez zasadę Agenta sieciowego, nie można ich modyfikować.

- **Szczegóły zainstalowanych aplikacji**

  Jeśli ta opcja jest włączona, informacje o aplikacjach zainstalowanych na urządzeniach klienckich są przesyłane do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dołącz informacje o poprawkach**

  Informacje o poprawkach aplikacji zainstalowanych na urządzeniach klienckich są wysyłane do Serwera administracyjnego. Włączenie tej opcji może zwiększyć obciążenie na Serwerze administracyjnym oraz DBMS, a także spowodować zwiększenie rozmiaru bazy danych.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

- **Szczegóły aktualizacji Windows Update**

  Jeśli ta opcja jest włączona, informacje o aktualizacjach Microsoft Windows Update, które powinny zostać zainstalowane na urządzeniach klienckich, są przesyłane do Serwera administracyjnego.

  Czasami, nawet wtedy, gdy opcja jest wyłączona, aktualizacje są wyświetlanie we właściwościach urządzenia w sekcji **Dostępne aktualizacje**. To może mieć miejsce, gdy, na przykład, urządzenia w organizacji zawierają luki, które mogłyby zostać wyeliminowane przez te aktualizacje.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

- **Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji**

  Jeśli ta opcja jest włączona, informacje o lukach w oprogramowaniu innej firmy (w tym oprogramowaniu firmy Microsoft), wykrytych na zarządzanych urządzeniach, oraz o aktualizacjach oprogramowania, które eliminują luki innych firm (nie dotyczy oprogramowania firmy Microsoft) są wysyłane do Serwera administracyjnego.

  Wybranie tej opcji (**Szczegóły luk w oprogramowaniu oraz odpowiednich aktualizacji)** zwiększy obciążenie sieci, obciążenie dysku Serwera administracyjnego oraz zużycie zasobów Agenta sieciowego.

  Domyślnie opcja ta jest włączona. Jest dostępny tylko dla systemu Windows.

  Aby zarządzać aktualizacjami oprogramowania firmy Microsoft, użyj opcji **Szczegóły aktualizacji Windows Update**.

- **Szczegóły rejestru sprzętu**

  Agent sieciowy zainstalowany na urządzeniu wysyła informacje o sprzęcie urządzenia do Serwera administracyjnego. Możesz przejrzeć szczegóły sprzętu we właściwościach urządzenia.

Aktualizacje oprogramowania i luki

W sekcji **Aktualizacje oprogramowania i luki** możesz skonfigurować wyszukiwanie i rozsyłanie aktualizacji systemu Windows, a także włączyć skanowanie plików wykonywalnych w poszukiwaniu luk. Ustawienia w sekcji **Aktualizacje oprogramowania i luki** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows:

- Użyj Serwera administracyjnego jako serwera WSUS

  Jeśli ta opcja jest włączona, aktualizacje systemu Windows są pobierane na Serwer administracyjny. Serwer administracyjny dostarcza pobrane aktualizacje usłudze Windows Update na urządzeniach klienckich w trybie scentralizowanym przy użyciu Agentów sieciowych.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie używany do pobierania aktualizacji systemu Windows. W tym przypadku urządzenia klienckie same pobierają aktualizacje systemu Windows.

  Domyślnie opcja ta jest wyłączona.

- Możesz ograniczyć aktualizacje systemu Windows, które użytkownicy mogą zainstalować na swoich urządzeniach ręcznie, korzystając z Windows Update.

  Na urządzeniach działających pod kontrolą systemu Windows 10, jeśli usługa Windows Update już wykryła aktualizacje dla urządzenia, nowa opcja, którą wybierzesz w sekcji **Zezwalaj użytkownikom na zarządzanie instalowaniem aktualizacji Windows Update**, zostaną zastosowane dopiero po zainstalowaniu wykrytych aktualizacji.

  Wybierz element z listy rozwijalnej:

  - Zezwalaj użytkownikom na instalację wszystkich dostępnych aktualizacji Windows Update

    Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach.

    Wybierz tę opcję, jeśli nie chcesz uczestniczyć w instalacji aktualizacji.

    Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

  - Zezwalaj użytkownikom na instalację wszystkich zatwierdzonych aktualizacji Windows Update

    Użytkownicy mogą zainstalować wszystkie aktualizacje Microsoft Windows Update, które są stosowane na ich urządzeniach i które zostały zatwierdzone przez Ciebie.

    Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych zatwierdzonych aktualizacji.

    Jeśli użytkownik ręcznie instaluje aktualizacje Microsoft Windows Update, aktualizacje mogą zostać pobrane z serwerów firmy Microsoft, a nie z Serwera administracyjnego. Jest to możliwe, jeśli Serwer administracyjny jeszcze nie pobrał tych aktualizacji. Pobieranie aktualizacji z serwerów Microsoft generuje dodatkowy ruch sieciowy.

  - Nie zezwalaj użytkownikom na instalowanie aktualizacji Windows Update

Użytkownicy nie mogą ręcznie zainstalować aktualizacji Microsoft Windows Update na swoich urządzeniach. Wszystkie stosowane aktualizacje są instalowane w sposób skonfigurowany przez Ciebie.

Wybierz tę opcję, jeśli chcesz zarządzać instalacją aktualizacji w sposób scentralizowany.

Na przykład, możesz chcieć zoptymalizować terminarz aktualizacji, aby sieć nie została przeciążona. Możesz skonfigurować terminarz aktualizacji po godzinach, aby nie przeszkadzały w pracy użytkowników.

- W grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** możesz wybrać tryb wyszukiwania aktualizacji:

  - **Aktywny**

    Jeśli ta opcja jest zaznaczona, Serwer administracyjny z pomocą Agenta sieciowego przesyła żądanie z Agenta Windows Update na urządzeniu klienckim do źródła uaktualnień: Serwery Windows Update lub WSUS. Następnie Agent sieciowy przesyła informacje z usługi Windows Update Agent do Serwera administracyjnego.

    Opcja zaczyna działać tylko wtedy, gdy zaznaczona jest opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

    Domyślnie opcja ta jest zaznaczona.

  - **Pasywny**

    Jeżeli ta opcja jest zaznaczona, Agent sieciowy co jakiś czas przesyła informacje od Serwera administracyjnego dotyczące aktualizacji pobranych przy ostatniej synchronizacji agenta usługi Windows Update ze źródłem uaktualnień. Jeśli nie zostanie przeprowadzona synchronizacja agenta usługi Windows Update ze źródłem uaktualnień, informacje o aktualizacjach Serwera administracyjnego będą przestarzałe.

    Wybierz tę opcję, jeśli chcesz uzyskać aktualizacje z pamięci podręcznej źródła uaktualnień.

  - **Wyłączone**

    Jeśli ta opcja jest zaznaczona, Serwer administracyjny nie żąda informacji dotyczących aktualizacji.

    Wybierz tę opcję, gdy, na przykład, chcesz najpierw przetestować aktualizacje na swoim lokalnym urządzeniu.

- **Skanuj pliki wykonywalne w poszukiwaniu luk podczas ich uruchamiania**

  Jeśli ta opcja jest włączona, pliki wykonywalne są skanowane w poszukiwaniu luk podczas ich uruchamiania.

  Domyślnie opcja ta jest włączona.

Zarządzanie ponownym uruchamianiem

W sekcji **Zarządzanie ponownym uruchamianiem** możesz określić działanie, jakie zostanie wykonane, jeśli system operacyjny musi być uruchomiony ponownie, gdy korzystasz, instalujesz lub dezinstalujesz aplikację. Ustawienia w sekcji **Zarządzanie ponownym uruchamianiem** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows:

- **Nie uruchamiaj ponownie systemu operacyjnego**

Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Jeżeli będzie to wymagane, automatycznie uruchom ponownie system operacyjny**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Wymuś restart po (min)**

    Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

    Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  - **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

Domyślnie opcja ta jest wyłączona.

Udostępnianie pulpitu Windows

W sekcji **Udostępnianie pulpitu Windows** możesz włączyć i skonfigurować audyt działań administratora wykonywanych na zdalnym urządzeniu podczas współdzielenia dostępu do pulpitu. Ustawienia w sekcji **Udostępnianie pulpitu Windows** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows:

- **Włącz audyt**

  Jeśli ta opcja jest włączona, audyt działań administratora na zdalnym urządzeniu jest włączony. Wpisy dotyczące działań administratora na zdalnym urządzeniu są zapisywane w:

  - Raporcie zdarzeń na zdalnym urządzeniu
  - W pliku z rozszerzeniem syslog, znajdującym się w folderze instalacyjnym Agenta sieciowego na zdalnym urządzeniu
  - W bazie danych zdarzeń programu Kaspersky Security Center

  Audyt działań administratora jest dostępny, gdy są spełnione następujące warunki:

  - Licencja Zarządzanie lukami i poprawkami jest w użyciu
  - Administrator posiada uprawnienie do włączania współdzielonego dostępu do pulpitu zdalnego urządzenia

  Jeśli ta opcja jest wyłączona, audyt działań administratora na zdalnym urządzeniu jest wyłączony.

  Domyślnie opcja ta jest wyłączona.

- **Maski plików, które będą monitorowane podczas odczytu**

  Lista zawiera maski plików. Jeśli audyt jest włączony, aplikacja monitoruje odczytywanie plików przez administratora, które odpowiadają maskom, i zapisuje informacje o odczycie plików. Lista jest dostępna, jeśli pole **Włącz audyt** jest zaznaczone. Możesz zmodyfikować maski plików i dodać nowe do listy. Każda nowa maska pliku powinna być określona na liście w nowym wierszu.

  Domyślnie określone są następujące maski plików:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Maski plików, które będą monitorowane podczas modyfikacji**

Lista zawiera maski plików na zdalnym urządzeniu. Jeśli audyt jest włączony, aplikacja monitoruje zmiany wprowadzone przez administratora w plikach, które odpowiadają maskom, i zapisuje informacje o tych modyfikacjach. Lista jest dostępna, jeśli pole **Włącz audyt** jest zaznaczone. Możesz zmodyfikować maski plików i dodać nowe do listy. Każda nowa maska pliku powinna być określona na liście w nowym wierszu.

Domyślnie określone są następujące maski plików:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Zarządzaj poprawkami i aktualizacjami

W sekcji **Zarządzaj poprawkami i aktualizacjami** możesz skonfigurować pobieranie i dystrybucję uaktualnień oraz instalację poprawek na zarządzanych urządzeniach:

- **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**

  Jeśli ta opcja jest włączona, poprawki Kaspersky ze stanem zatwierdzenia *Niezdefiniowane* będą automatycznie instalowane na zarządzanych urządzeniach natychmiast po pobraniu z serwerów aktualizacji.

  Jeśli ta opcja jest wyłączona, poprawki Kaspersky, które zostały pobrane i oznaczone jako *Niezdefiniowane*, zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzone*.

  Domyślnie opcja ta jest włączona.

- **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)**

  Jeśli ta opcja jest włączona, tryb offline pobierania uaktualnień jest używany. Jeśli Serwer administracyjny pobierze uaktualnienia, powiadomi Agenta sieciowego (na urządzeniach, na których jest zainstalowany) o uaktualnieniach, które będą wymagane dla zarządzanych aplikacji. Jeśli Agent sieciowy otrzyma informacje o tych uaktualnieniach, pobierze odpowiednie pliki z Serwera administracyjnego z wyprzedzeniem. Przy pierwszym nawiązaniu połączenia z Agentem sieciowym, Serwer administracyjny inicjuje pobranie uaktualnień. Jeśli Agent sieciowy pobierze wszystkie uaktualnienia na urządzenie klienckie, staną się one dostępne dla aplikacji na tym urządzeniu.

  Jeśli zarządzana aplikacja na urządzeniu klienckim spróbuje uzyskać dostęp do Agenta sieciowego w celu uzyskania uaktualnień, Agent sieciowy sprawdzi, czy posiada wszystkie wymagane uaktualnienia. Jeśli uaktualnienia zostały pobrane z Serwera administracyjnego nie więcej niż 25 godzin przed zażądaniem ich przez zarządzaną aplikację, Agent sieciowy nie nawiąże połączenia z Serwerem administracyjnym, ale dostarczy zarządzanej aplikacji uaktualnienia z lokalnej pamięci podręcznej. Połączenie z Serwerem administracyjnym może nie zostać nawiązane, gdy Agent sieciowy dostarcza uaktualnienia aplikacji na urządzeniach klienckich, ale połączenie nie jest wymagane w celu przeprowadzenia aktualizacji.

  Jeśli ta opcja jest wyłączona, tryb offline pobierania uaktualnień nie jest używany. Uaktualnienia są rozsyłane zgodnie z terminarzem zadania pobierania uaktualnień.

  Domyślnie opcja ta jest włączona.

Łączność

Sekcja **Łączność** zawiera trzy podsekcje:

- **Sieć**
- **Profile połączenia**
- **Terminarz połączeń**

W podsekcji **Sieć** możesz skonfigurować połączenie z Serwerem administracyjnym, włączyć korzystanie z portu UDP oraz określić numer UDP.

- W grupie ustawień **Połącz z Serwerem administracyjnym** możesz skonfigurować połączenie z serwerem administracyjnym oraz określić przedziału czasu dla synchronizacji pomiędzy urządzeniami klienckimi a serwerem administracyjnym:

  - Okres synchronizacji (min)

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

    Jeśli okres synchronizacji wynosi mniej niż 15 minut, synchronizacja odbywa się co każde 15 minut. Jeśli okres synchronizacji jest ustawiony na 15 minut lub więcej, synchronizacja odbywa się w określonym przedziale synchronizacji.

  - Kompresuj ruch sieciowy

    Jeżeli ta opcja jest włączona, prędkość transferu danych przez Agenta sieciowego zostaje zwiększona poprzez zmniejszenie ilości przesyłanych informacji i tym samym zmniejszenie obciążenia Serwera administracyjnego.

    Obciążenie procesora komputera klienckiego może się zwiększyć.

    Domyślnie pole to jest zaznaczone.

  - Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows

    Jeżeli ta opcja jest włączona, port UDP, niezbędny do pracy Agenta sieciowego, zostanie dodany do listy wykluczeń Zapory systemu Microsoft Windows.

    Domyślnie opcja ta jest włączona.

  - Użyj połączenia SSL

    Jeśli ta opcja jest włączona, połączenie z Serwerem administracyjnym jest nawiązywane poprzez bezpieczny port przy użyciu protokołu SSL.

    Domyślnie opcja ta jest włączona.

  - Użyj bramy połączenia na punkcie dystrybucji (jeśli jest dostępny) w domyślnych ustawieniach połączenia

    Jeśli ta opcja jest włączona, brama połączenia na punkcie dystrybucji jest używana z ustawieniami określonymi we właściwościach grupy administracyjnej.

    Domyślnie opcja ta jest włączona.

- Użyj portu UDP

  Jeśli chcesz, żeby zarządzane urządzenia nawiązywały połączenie z serwerem KSN proxy poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

- **Numer portu UDP**

  W tym polu możesz wprowadzić numer portu UDP. Domyślny numer portu to 15000.

  Używany jest system dziesiętny.

  Jeżeli na urządzeniu klienckim zainstalowany jest system Windows XP Service Pack 2, wówczas wbudowana zapora sieciowa będzie blokowała port UDP o numerze 15000. Port ten należy otworzyć ręcznie.

- **Użyj punktu dystrybucji, aby wymusić połączenie z Serwerem administracyjnym**

  Wybierz tę opcję, jeśli w oknie ustawień punktu dystrybucji zaznaczyłeś opcję **Użyj tego punktu dystrybucji jako serwera push**. W przeciwnym razie punkt dystrybucji nie będzie działał jako serwer push.

W podsekcji **Profile połączenia** możesz określić ustawienia lokalizacji sieciowej i włączyć tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny. Ustawienia w sekcji **Profile połączenia** są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows i macOS:

- **Ustawienia lokalizacji sieciowej**

  Ustawienia lokalizacji sieciowej definiują cechy sieci, do której podłączone jest urządzenie klienckie, i określają reguły przełączania Agenta sieciowego z jednego profilu połączenia Serwera administracyjnego do innego, gdy te cechy sieci zostaną zmienione.

- **Profile połączeń Serwera administracyjnego**

  W tej sekcji możesz dodawać i wyświetlać profile połączenia Agenta sieciowego z Serwerem administracyjnym. W tej sekcji możesz także utworzyć reguły przełączania Agenta sieciowego na inne Serwery administracyjne, gdy wystąpią następujące zdarzenia:

  - Gdy urządzenie klienckie zostanie podłączone do innej sieci lokalnej
  - Gdy zostanie zerwane połączenie między urządzeniem a siecią lokalną organizacji
  - Gdy adres bramy połączenia zostanie zmieniony lub adres serwera DNS zostanie zmodyfikowany

  Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

- **Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny**

  Jeśli ta opcja jest włączona, w przypadku połączenia przez ten profil, aplikacje zainstalowane na urządzeniu klienckim będą używać profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie opcja ta jest wyłączona.

W podsekcji **Terminarz połączeń** możesz określić przedziały czasu, w trakcie których Agent sieciowy wysyła dane do Serwera administracyjnego:

- **Połącz, gdy jest to konieczne**

Jeśli ta opcja jest zaznaczona, połączenie jest nawiązywane, gdy Agent sieciowy musi wysłać dane na Serwer administracyjny.

Domyślnie opcja ta jest zaznaczona.

- **Połącz w określonych przedziałach czasu**

  Jeśli ta opcja jest zaznaczona, Agent sieciowy łączy się z Serwerem administracyjnym w określonym czasie. Możesz dodać kilka przedziałów czasu.

Przeszukiwanie sieci według punktów dystrybucji

W sekcji **Przeszukiwanie sieci według punktów dystrybucji** możesz skonfigurować automatyczne przeszukiwanie sieci. Ustawienia przeszukiwania są dostępne tylko na urządzeniach działających pod kontrolą systemu Windows. W celu włączenia przeszukiwania sieci i skonfigurowania jego częstotliwości możesz użyć następujących opcji:

- **Sieć Windows**

  Jeśli ta opcja jest włączona, Serwer administracyjny automatycznie przeszuka sieć zgodnie z terminarzem skonfigurowanym po kliknięciu odnośników **Ustaw terminarz szybkiego przeszukiwania** i **Ustaw terminarz pełnego przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie przeszukiwał sieci.

  Interwał wykrywania urządzeń dla Agenta sieciowego w wersjach przed 10.2 może zostać skonfigurowany w polach **Częstotliwość pobierania informacji z domen Windows (min)** i **Częstotliwość przeszukiwania sieci (min)**. Pola są dostępne, jeśli opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

- **Zeroconf**

  Jeśli ta opcja jest włączona, punkt dystrybucji automatycznie przeszukuje sieć za pomocą urządzeń IPv6, używając zero-configuration networking (zwany również *Zeroconf*). W takim przypadku włączone przeszukiwanie zakresu adresów IP jest ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć.

  W celu rozpoczęcia korzystania z Zeroconf, muszą być spełnione następujące warunki:

  - Punkt dystrybucji musi działać pod systemem Linux.
  - Musisz zainstalować narzędzie avahi-browse na punkcie dystrybucji.

  Jeśli ta opcja jest wyłączona, punkt dystrybucji nie przeszukuje sieci z urządzeniami IPv6.

  Domyślnie opcja ta jest wyłączona.

- **Zakresy IP**

  Jeśli opcja jest włączona, Serwer administracyjny automatycznie przeszuka zakresy IP zgodnie z terminarzem skonfigurowanym po kliknięciu odnośnika **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie przeszukiwał zakresów IP.

  Częstotliwość przeszukiwania zakresu IP dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

- Active Directory

  Jeśli ta opcja jest włączona, Serwer administracyjny automatycznie przeszuka Active Directory zgodnie z terminarzem skonfigurowanym po kliknięciu odnośnika **Ustaw terminarz przeszukiwania**.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny nie będzie przeszukiwał Active Directory.

  Częstotliwość przeszukiwania Active Directory dla Agenta sieciowego w wersjach poprzedzających 10.2 może być skonfigurowana w polu **Interwał przeszukiwania (min)**. Pole jest dostępne, jeśli ta opcja jest włączona.

  Domyślnie opcja ta jest wyłączona.

Ustawienia sieci dla punktów dystrybucji

W sekcji **Ustawienia sieci dla punktów dystrybucji** możesz określić ustawienia dostępu do internetu:

- **Użyj serwera proxy**
- **Adres**
- **Numer portu**
- Pomiń serwer proxy dla adresów lokalnych

  Jeśli ta opcja jest włączona, żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

  Domyślnie opcja ta jest wyłączona.

- Uwierzytelnianie na serwerze proxy

  Jeśli to pole jest włączone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  Domyślnie, pole to jest wyłączone.

- **Nazwa użytkownika**
- **Hasło**

KSN Proxy (punkty dystrybucji)

W sekcji **KSN Proxy (punkty dystrybucji)** możesz skonfigurować aplikację tak, aby używała punktu dystrybucji do przekazywania żądań Kaspersky Security Network (KSN) z zarządzanych urządzeń:

- Włącz KSN Proxy po stronie punktu dystrybucji

Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky. Domyślnie, Oświadczenie KSN znajduje się w %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

- **Przesyłaj żądania KSN do Serwera administracyjnego**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dostęp do KSN Cloud/Private KSN bezpośrednio przez Internet**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub Private KSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub Private KSN.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej), nie może uzyskać bezpośredniego dostępu do Private KSN. Jeśli chcesz ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do prywatnej sieci KSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 12 (lub późniejszej), może uzyskać bezpośredni dostęp do Private KSN.

- **Port**

  Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

- **Port UDP**

  Jeśli chcesz, żeby zarządzane urządzenia nawiązywały połączenie z serwerem KSN proxy poprzez port UDP, włącz opcję **Użyj portu UDP** i określ **numer portu UDP**. Domyślnie opcja ta jest włączona. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

Aktualizacje (punkty dystrybucji)

W sekcji **Aktualizacje (punkty dystrybucji)** możesz włączyć funkcję pobierania plików diff, dzięki czemu punkty dystrybucji pobierają aktualizacje w postaci plików diff z serwerów aktualizacji firmy Kaspersky.

Historia rewizji

Na tej zakładce możesz przejrzeć listę rewizji zasady i wycofać zmiany wprowadzone do zasady (jeśli to konieczne).

Porównanie ustawień zasady Agenta sieciowego według systemów operacyjnych

Poniższa tabela pokazuje, jakich ustawień zasady Agenta sieciowego możesz użyć do skonfigurowania Agenta sieciowego z określonym systemem operacyjnym.

Ustawienia zasady Agenta sieciowego: porównanie według systemów operacyjnych

Sekcja Zasada	Windows	macOS	Linux
Ogólne	✓	✓	✓
Konfiguracja zdarzenia	✓	✓	✓
Ustawienia	✓	✓	✓ Dostępne są tylko opcje **Maksymalny rozmiar kolejki zdarzeń, w MB** oraz **Aplikacja może pobierać rozszerzone dane zasad na urządzenie**.
Repozytoria	✓	–	✓ Dostępne są tylko opcje **Szczegóły zainstalowanych aplikacji** i **Szczegóły rejestru sprzętu**.
Aktualizacje oprogramowania i luki	✓	–	–
Zarządzanie ponownym uruchamianiem	✓	–	–
Udostępnianie pulpitu Windows	✓	–	–
Zarządzaj poprawkami i aktualizacjami	✓	–	–
Łączność → Sieć	✓	✓	✓ Za wyjątkiem opcji **Otwórz porty dla Agenta sieciowego w Zaporze systemu Windows**.
Łączność → Profile połączenia	✓	✓	–
Łączność → Terminarz połączeń	✓	✓	✓
Przeszukiwanie sieci według punktów dystrybucji	✓ Dostępne są tylko opcje **Sieć Windows**, **Zakresy IP** oraz **Active Directory**.	–	✓ Dostępne są tylko opcje **Zeroconf** oraz **Zakresy IP**.
Ustawienia sieci dla punktów dystrybucji	✓	✓	✓

KSN Proxy (punkty dystrybucji)	✓	–	✓
Aktualizacje (punkty dystrybucji)	✓	–	✓
Historia rewizji	✓	✓	✓

Ręczna konfiguracja zasady Kaspersky Endpoint Security

Ta sekcja zawiera zalecenia dotyczące konfigurowania profilu Kaspersky Endpoint Security. Możesz przeprowadzić konfigurację w oknie właściwości zasady. Podczas edytowania ustawienia kliknij ikonę kłódki po prawej stronie odpowiedniej grupy ustawień, aby zastosować określone wartości do stacji roboczej.

Konfigurowanie Kaspersky Security Network

Kaspersky Security Network (KSN) to infrastruktura usług w chmurze, która zawiera informacje o reputacji plików, zasobach sieciowych i oprogramowaniu. Kaspersky Security Network umożliwia Kaspersky Endpoint Security for Windows szybsze reagowanie na różnego rodzaju zagrożenia, zwiększa wydajność komponentów ochrony i zmniejsza prawdopodobieństwo fałszywych trafień. Więcej informacji na temat Kaspersky Security Network można znaleźć w Pomocy Kaspersky Endpoint Security for Windows.

W celu określenia zalecanych ustawień KSN:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Zaawansowana ochrona przed zagrożeniami** → **Kaspersky Security Network**.
4. Upewnij się, że opcja **Użyj KSN Proxy** jest włączona. Użyj tej opcji do redystrybucji i optymalizacji ruchu w sieci.
5. [Opcjonalne] Włącz korzystanie z serwerów KSN, jeśli usługa KSN proxy jest niedostępna. Serwery KSN mogą znajdować się po stronie Kaspersky (jeśli używana jest Global KSN) lub po stronie firm trzecich (jeśli używana jest Private KSN).
6. Kliknij **OK**.

   Zostaną określone zalecane ustawienia KSN.

Sprawdzanie listy sieci chronionych przez Zaporę sieciową

Upewnij się, że Kaspersky Endpoint Security for Windows Firewall chroni wszystkie Twoje sieci. Domyślnie Zapora sieciowa chroni sieci z następującymi typami połączeń:

- **Sieć publiczna**. Aplikacje antywirusowe, zapory ogniowe czy filtry nie chronią urządzeń w takiej sieci.
- **Sieć lokalna**. Dostęp do plików i drukarek jest ograniczony dla urządzeń w tej sieci.
- **Zaufana sieć**. Urządzenia w takiej sieci są chronione przed atakami oraz nieautoryzowanym dostępem do plików i danych.

Jeśli skonfigurowano niestandardową sieć, upewnij się, że zapora sieciowa ją chroni. W tym celu sprawdź listę sieci we właściwościach Kaspersky Endpoint Security for Windows. Lista może nie zawierać wszystkich sieci.

Więcej informacji na temat Zapory sieciowej można znaleźć w Pomocy Kaspersky Endpoint Security for Windows.

W celu sprawdzenia listy sieci:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
4. Pod sekcją **Dostępne sieci** kliknij odnośnik **Ustawienia sieci**.

   Zostanie otwarte okno **Połączenia sieciowe**. To okno będzie wyświetlało listę sieci.
5. Jeśli na liście brakuje sieci, dodaj ją.

Wyłączanie skanowania urządzeń sieciowych

Gdy Kaspersky Endpoint Security for Windows skanuje dyski sieciowe, może to spowodować ich znaczne obciążenie. Praktyczniejsze jest wykonywanie bezpośredniego skanowania na serwerach plików.

Możesz wyłączyć skanowanie dysków sieciowych we właściwościach Kaspersky Endpoint Security for Windows. Opis tych właściwości profilu znajduje się w Pomocy Kaspersky Endpoint Security for Windows.

W celu wyłączenia skanowania dysków sieciowych:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
4. W sekcji **Obszar ochrony** wyłącz opcję **Wszystkie dyski sieciowe**.
5. Kliknij **OK**.

Skanowanie dysków sieciowych zostanie wyłączone.

Wykluczanie szczegółów oprogramowania z pamięci Serwera administracyjnego

Zalecamy, aby Serwer administracyjny nie zapisywał informacji o modułach oprogramowania uruchamianych na urządzeniach sieciowych. W rezultacie pamięć Serwera administracyjnego nie jest przepełniona.

Możesz wyłączyć zapisywanie tych informacji we właściwościach Kaspersky Endpoint Security for Windows.

W celu wyłączenia zapisywania informacji o zainstalowanych modułach oprogramowania:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Ustawienia ogólne** → **Raporty i pliki danych**.
4. Pod sekcją **Przesyłanie danych do Serwera administracyjnego** wyłącz pole **Informacje o uruchomionych aplikacjach**, jeśli wciąż jest włączone w zasadzie najwyższego poziomu.

   Jeśli to pole jest włączone, bazy danych Serwera administracyjnego zapisują informacje o wszystkich wersjach wszystkich modułów oprogramowania na urządzeniach w sieci. Informacje mogą wymagać znaczącej ilości miejsca na dysku dla bazy danych Kaspersky Security Center (kilkadziesiąt gigabajtów).

Informacje o zainstalowanych modułach oprogramowania nie są już zapisywane w bazie danych Serwera administracyjnego.

Konfigurowanie dostępu do interfejsu Kaspersky Endpoint Security for Windows na stacjach roboczych

Jeśli ochrona antywirusowa w sieci organizacji musi być zarządzana w trybie scentralizowanym poprzez Kaspersky Security Center, określ ustawienia interfejsu we właściwościach Kaspersky Endpoint Security for Windows, jak opisano poniżej. W rezultacie zapobiegniesz nieautoryzowanemu dostępowi do Kaspersky Endpoint Security for Windows na stacjach roboczych i zmianie ustawień Kaspersky Endpoint Security for Windows.

Opis tych właściwości profilu znajduje się w Pomocy Kaspersky Endpoint Security for Windows.

W celu określenia zalecanych ustawień interfejsu:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.

   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady przejdź do **Ustawienia aplikacji** → **Ustawienia ogólne** → **Interfejs**.
4. Pod sekcją **Interakcja z użytkownikiem** wybierz opcję **Bez interfejsu**. To wyłącza wyświetlanie interfejsu użytkownika Kaspersky Endpoint Security for Windows na stacjach roboczych, więc ich użytkownicy nie mogą zmieniać ustawień Kaspersky Endpoint Security for Windows.

5. Pod sekcją **Ochrona hasłem** włącz przycisk przełącznika. Zmniejszy to ryzyko nieautoryzowanych lub niezamierzonych zmian w ustawieniach Kaspersky Endpoint Security for Windows na stacjach roboczych.

Zalecane ustawienia dla interfejsu Kaspersky Endpoint Security for Windows zostały określone.

Zapisywanie ważnych zdarzeń dot. zasad w bazie danych Serwera administracyjnego

Aby uniknąć przepełnienia bazy danych Serwera administracyjnego, zalecane jest zapisywanie tylko ważnych zdarzeń w bazie danych.

W celu skonfigurowania rejestracji ważnych zdarzeń w bazie danych Serwera administracyjnego:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij zasadę dla Kaspersky Endpoint Security for Windows.
   Zostanie otwarte okno właściwości wybranej zasady.
3. We właściwościach zasady otwórz zakładkę **Konfiguracja zdarzenia**.
4. W sekcji **Krytyczny** kliknij **Dodaj zdarzenie** i zaznacz pola tylko obok następujących zdarzeń:
   - *Uwaga! Sprawdź licencję*
   - *Automatyczne uruchamianie aplikacji jest wyłączone*
   - *Błąd aktywacji*
   - *Wykryto aktywne zagrożenie Należy uruchomić zaawansowane leczenie*
   - *Leczenie nie jest możliwe*
   - *Wykryto wcześniej otwarty niebezpieczny odnośnik*
   - *Proces został przerwany*
   - *Zablokowano aktywność sieciową*
   - *Wykryto atak sieciowy*
   - *Zablokowano uruchomienie aplikacji*
   - *Dostęp zabroniony (bazy lokalne)*
   - *Dostęp zabroniony (KSN)*
   - *Błąd aktualizacji lokalnej*
   - *Nie można uruchomić dwóch zadań jednocześnie*
   - *Błąd interakcji z Kaspersky Security Center*

- *Nie wszystkie komponenty zostały zaktualizowane*
- *Błąd zastosowania reguł szyfrowania/deszyfrowania pliku*
- *Błąd włączenia trybu przenośnego*
- *Błąd wyłączenia trybu przenośnego*
- *Nie można załadować modułu szyfrującego*
- *Nie można zastosować profilu*
- *Błąd zmiany komponentów aplikacji*

5. Kliknij **OK**.
6. W sekcji **Błąd funkcjonalny** kliknij **Dodaj zdarzenie** i zaznacz pole wyboru obok zdarzenia *Nieprawidłowe ustawienia zadania. Ustawienia nie zostały zastosowane*.
7. Kliknij **OK**.
8. W sekcji **Ostrzeżenie** kliknij **Dodaj zdarzenie** i zaznacz pola tylko obok następujących zdarzeń:
   - *Autoochrona jest wyłączona*
   - *Składniki ochrony są wyłączone*
   - *Nieprawidłowy klucz zapasowy*
   - *Zostało wykryte legalne oprogramowanie, które może zostać użyte do wyrządzenia szkody na komputerze lub uszkodzić dane osobiste (bazy lokalne)*
   - *Zostało wykryte legalne oprogramowanie, które może zostać użyte do wyrządzenia szkody na komputerze lub uszkodzić dane osobiste (KSN)*
   - *Usunięty obiekt*
   - *Wyleczony obiekt*
   - *Użytkownik zrezygnował z profilu szyfrowania*
   - *Plik przywrócony z Kwarantanny KATA*
   - *Plik przeniesiony do Kwarantanny KATA*
   - *Wiadomość o zablokowaniu uruchomienia aplikacji do administratora*
   - *Wiadomość o zablokowaniu dostępu do urządzenia do administratora*
   - *Wiadomość o zablokowaniu dostępu do strony internetowej do administratora*
9. Kliknij **OK**.
10. W sekcji **Informacja** kliknij **Dodaj zdarzenie** i zaznacz pola tylko obok następujących zdarzeń:
    - *Została utworzona kopia zapasowa obiektu*

- *Zablokowane uruchomienie aplikacji w trybie testowym*

11. Kliknij **OK**.

Zostanie skonfigurowana rejestracja ważnych zdarzeń w bazie danych Serwera administracyjnego.

Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security

Optymalną i zalecaną opcją terminarza dla Kaspersky Endpoint Security jest **Po pobraniu nowych aktualizacji do repozytorium**, gdy zaznaczone jest pole **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Udzielanie dostępu offline urządzeniu zewnętrznemu, zablokowanemu przez Kontrolę urządzeń

W komponencie Kontrola urządzeń zasady Kaspersky Endpoint Security for Windows możesz zarządzać dostępem użytkownika do urządzeń zewnętrznych, które są instalowane na lub podłączane do urządzenia klienckiego (na przykład: dyski twarde, aparaty lub moduły Wi-Fi). To umożliwia ochronę urządzenia klienckiego przed infekcją, gdy podłączone są takie urządzenia zewnętrzne, oraz zapobiega utracie lub wyciekowi danych.

Jeśli chcesz udzielić tymczasowego dostępu do urządzenia zewnętrznego, zablokowanego przez Kontrolę urządzeń, ale nie jest możliwe dodanie urządzenia do listy zaufanych urządzeń, możesz udzielić tymczasowego dostępu offline do urządzenia zewnętrznego. Dostęp offline oznacza, że urządzenie klienckie nie ma dostępu do sieci.

Możesz przyznać dostęp w trybie offline do urządzenia zewnętrznego zablokowanego przez Kontrolę urządzeń tylko wtedy, gdy opcja **Zezwól na żądanie tymczasowego dostępu** jest włączona w ustawieniach Kaspersky Endpoint Security for Windows, w sekcji **Ustawienia aplikacji** → **Kontrola bezpieczeństwa** → Kontrola **urządzeń**.

Udzielanie dostępu offline urządzeniu zewnętrznemu, zablokowanemu przez Kontrolę urządzeń obejmuje następujące etapy:

1. W oknie dialogowym Kaspersky Endpoint Security for Windows użytkownik urządzenia, który chce mieć dostęp do zablokowanego urządzenia zewnętrznego, wygeneruj plik prośby o dostęp i wyślij go do administratora Kaspersky Security Center.

2. Po otrzymaniu tego zgłoszeni, administrator Kaspersky Security Center tworzy plik klucza dostępu i wysyła go do użytkownika.

3. W oknie dialogowym Kaspersky Endpoint Security for Windows użytkownik urządzenia aktywuje plik klucza dostępu i uzyskuje tymczasowy dostęp do urządzenia zewnętrznego.

W celu udzielenia tymczasowego dostępu do urządzenia zewnętrznego, zablokowanego przez Kontrolę urządzeń:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na tej liście wybierz urządzenie użytkownika, który żąda dostępu do urządzenia zewnętrznego zablokowanego przez Kontrolę urządzeń.

   Możesz wybrać tylko jedno urządzenie.

3. Nad listą zarządzanych urządzeń kliknij ikonę, a następnie kliknij owalny przycisk (...) **Udziel dostępu do urządzenia w trybie offline**.

4. W otwartym oknie **Ustawienia aplikacji**, w sekcji **Kontrola urządzeń** kliknij przycisk **Przeglądaj**.

5. Wybierz plik żądania dostępu otrzymany od użytkownika, a następnie kliknij przycisk **Otwórz**. Plik powinien mieć format AKEY.

   Zostaną wyświetlone szczegóły dotyczące zablokowanego urządzenia, do którego o dostęp poprosił użytkownik.

6. Określ wartość ustawienia **Czas trwania dostępu**.

   To ustawienie definiuje długość czasu, na jaki udzielasz użytkownikowi dostępu do zablokowanego urządzenia. Domyślna wartość to wartość, która została określona przez użytkownika podczas tworzenia pliku żądania dostępu.

7. Określ wartość ustawienia **Okres aktywacji**.

   To ustawienie definiuje przedział czasu, w trakcie którego użytkownik może aktywować dostęp do zablokowanego urządzenia przy użyciu dostarczonego klucza dostępu.

8. Kliknij przycisk **Zapisz**.

   Spowoduje to otwarcie standardowego okna **Zapisz klucz dostępu**.

9. Wybierz folder docelowy, w którym chcesz zapisać plik zawierający klucz dostępu dla zablokowanego urządzenia.

10. Kliknij przycisk **Zapisz**.

    W rezultacie, po wysłaniu do użytkownika pliku klucza dostępu i aktywowaniu go przez użytkownika w oknie dialogowym Kaspersky Endpoint Security for Windows, użytkownik posiada tymczasowy dostęp do zablokowanego urządzenia dla określonego przedziału czasu.

Zdalne usuwanie aplikacji lub aktualizacji oprogramowania

W celu zdalnego usunięcia aplikacji lub aktualizacji oprogramowania z wybranych urządzeń:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Zdalna dezinstalacja aplikacji**.

4. Określ nazwę tworzonego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).

5. Wybierz urządzenia, do których zadanie zostanie przypisane.

6. Wybierz rodzaj oprogramowania, które chcesz usunąć, a następnie wybierz określone aplikacje, aktualizacje lub łaty, które chcesz usunąć:

   - **Odinstaluj zarządzane aplikacje**

     Zostanie wyświetlona lista aplikacji Kaspersky. Wybierz aplikację, którą chcesz usunąć.

   - **Odinstaluj niekompatybilną aplikację**

     Zostanie wyświetlona lista aplikacji niekompatybilnych z aplikacjami zabezpieczającymi firmy Kaspersky lub Kaspersky Security Center. Zaznacz pola obok aplikacji, które chcesz usunąć.

   - **Odinstaluj aplikację z rejestru aplikacji**

Domyślnie, Agenty sieciowe wysyłają do Serwera administracyjnego informacje o aplikacjach zainstalowanych na zarządzanych urządzeniach. Lista zainstalowanych aplikacji jest przechowywana w rejestrze aplikacji.

W celu wybrania aplikacji z rejestru aplikacji:

a. Kliknij pole **Aplikacja do odinstalowania**, a następnie wybierz aplikację, którą chcesz usunąć.

b. Określ opcje dezinstalacji:

- Tryb dezinstalacji

  Wybierz sposób dezinstalacji aplikacji:

  - **Określ polecenie dezinstalacji automatycznie**

    Jeśli aplikacja posiada polecenie dezinstalacji zdefiniowane przez producenta aplikacji, Kaspersky Security Center użyje tego polecenia. Nie jest zalecane wybranie tej opcji.

  - **Określ polecenie dezinstalacji**

    Wybierz tę opcję, jeśli chcesz określić swoje polecenie do dezinstalacji aplikacji.

    W pierwszej kolejności zalecane jest usunięcie aplikacji przy użyciu opcji **Określ polecenie dezinstalacji automatycznie**. Jeśli dezinstalacja za pośrednictwem automatycznie zdefiniowanego polecenia nie powiedzie się, wówczas użyj swojego polecenia.

    W polu wpisz polecenie instalacji, a następnie określ następującą opcję:

    Użyj tego polecenia do dezinstalacji, dopóki nie zostanie ono wykryte automatycznie

    Kaspersky Security Center sprawdza, czy wybrana aplikacja posiada polecenie dezinstalacji zdefiniowane przez producenta aplikacji. Jeśli polecenie zostało wykryte, Kaspersky Security Center użyje go zamiast polecenia określonego w polu **Polecenie do dezinstalacji aplikacji**.

    Nie jest zalecane włączenie tej opcji.

- Wykonaj ponowne uruchomienie po pomyślnym odinstalowaniu aplikacji

  Jeśli po pomyślnej dezinstalacji aplikacji wymagane jest ponowne uruchomienie systemu operacyjnego na zarządzanym urządzeniu, system operacyjny zostanie automatycznie uruchomiony ponownie.

- Odinstaluj wybraną aktualizację aplikacji, poprawkę lub aplikację firmy trzeciej

Zostanie wyświetlona lista aktualizacji, łat i aplikacji innych firm. Wybierz element, który chcesz usunąć.

Wyświetlona lista jest ogólną listą aplikacji i aktualizacji i nie odpowiada aplikacjom i aktualizacjom zainstalowanym na zarządzanych urządzeniach. Przed wybraniem elementu zalecane jest zapewnienie, że aplikacja lub aktualizacja jest zainstalowana na urządzeniu zdefiniowanym w obszarze zadania. Listę urządzeń, na których aplikacja lub aktualizacja została zainstalowana, możesz przejrzeć w oknie właściwości.

W celu wyświetlenia listy urządzeń:

a. Kliknij nazwę aplikacji lub aktualizacji.

Zostanie otwarte okno właściwości.

b. Otwórz sekcję **Urządzenia**.

Listę zainstalowanych aplikacji i aktualizacji możesz przejrzeć także w oknie właściwości urządzenia.

7. Określ sposób, w jaki urządzenia klienckie pobiorą narzędzie do dezinstalacji:

- **Przy użyciu Agenta sieciowego**

  Pliki są dostarczane do urządzeń klienckich przez Agenta sieciowego zainstalowanego na tych urządzeniach klienckich.

  Jeśli ta opcja została wyłączona, pliki zostaną dostarczone przy użyciu narzędzi Microsoft Windows.

  Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń, na których zainstalowano Agenty sieciowe.

- **Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny**

  Pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego Serwera administracyjnego. Możesz włączyć tę opcję, jeśli na urządzeniu klienckim nie ma zainstalowanego Agenta sieciowego, ale urządzenie klienckie jest w tej samej sieci, co Serwer administracyjny.

- **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**

  Pliki są przesyłane do urządzeń klienckich przy użyciu narzędzi systemu operacyjnego za pośrednictwem punktów dystrybucyjny. Możesz włączyć tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny.

  Jeśli opcja **Przy użyciu Agenta sieciowego** jest włączona, pliki będą dostarczane przy użyciu narzędzi systemu operacyjnego, jeśli narzędzia Agenta sieciowego będą niedostępne.

- **Maksymalna liczba jednoczesnych pobierań**

  Maksymalna dozwolona liczba urządzeń klienckich, do których Serwer administracyjny może jednocześnie przesłać pliki. Im większa ta liczba, tym szybciej aplikacja zostanie odinstalowana, ale obciążenie na Serwerze administracyjnym jest większe.

- **Maksymalna liczba prób dezinstalacji**

Jeśli podczas wykonywania zadania *Zdalna dezinstalacja aplikacji* programowi Kaspersky Security Center nie uda się zainstalować aplikacji na zarządzanym urządzeniu w obrębie liczby uruchomień instalatora określonych przez parametr, Kaspersky Security Center zatrzyma dostarczanie narzędzia do dezinstalacji na to zarządzane urządzenie i już nie uruchomi instalatora na urządzeniu.

Parametr **Maksymalna liczba prób dezinstalacji** umożliwia zachowanie zasobów zarządzanego urządzenia, a także zmniejszyć ruch sieciowy (dezinstalacja, uruchomienie pliku MSI i wiadomości o błędach).

Powtarzające się próby uruchomienia zadania mogą wskazywać na problem na urządzeniu i uniemożliwiać przeprowadzenie dezinstalacji. Administrator powinien rozwiązać problem w określonej liczbie prób dezinstalacji, a następnie uruchomić zadanie ponownie (ręcznie lub zgodnie z terminarzem).

Jeśli dezinstalacja się nie powiedzie, problem jest uznawany za nierozwiązalny i wszelkie dalsze uruchomienia zadania są postrzegane jako niepotrzebne zużywanie zasobów i ruchu sieciowego.

Po utworzeniu zadania, licznik prób jest ustawiony na `0`. Każde uruchomienie instalatora, które zwraca błąd na urządzeniu, zwiększa wartość licznika o jeden.

Jeśli liczba prób określonych w parametrze została przekroczona, a urządzenie jest gotowe do odinstalowania aplikacji, możesz zwiększyć wartość parametru **Maksymalna liczba prób dezinstalacji** i uruchomić zadanie do odinstalowania aplikacji. W razie czego możesz utworzyć nowe zadanie *Zdalna dezinstalacja aplikacji*.

- Zweryfikuj rodzaj systemu operacyjnego przed pobraniem

  Przed przesłaniem plików na urządzenia klienckie program Kaspersky Security Center sprawdza, czy ustawienia narzędzia do instalacji są stosowane do systemu operacyjnego urządzenia klienckiego. Jeśli ustawienia nie są stosowane, Kaspersky Security Center nie przesyła plików i nie próbuje zainstalować aplikacji. Na przykład, aby zainstalować aplikację Windows na urządzenia grupy administracyjnej, która zawiera urządzenia działające pod kontrolą różnych systemów operacyjnych, możesz przypisać zadanie instalacji do grupy administracyjnej, a następnie włączyć tę opcję, aby pominąć urządzenia, na których jest uruchomiony system operacyjny inny niż Windows.

8. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

- Nie uruchamiaj ponownie urządzenia

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- Uruchom urządzenie ponownie

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- Pytaj użytkownika o akcję

Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

9. Jeśli to konieczne, dodaj konta, które będą używane do uruchamiania zadania zdalnej dezinstalacji:

- **Konto nie jest wymagane (Agent sieciowy jest zainstalowany)**

  Jeśli ta opcja jest zaznaczona, nie musisz określić konta, z poziomu którego zostanie uruchomiony instalator aplikacji. Zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

  Jeśli Agent sieciowy nie został zainstalowany na urządzeniach klienckich, ta opcja nie będzie dostępna.

- **Konto wymagane (Agent sieciowy nie jest używany)**

Wybierz tę opcję, jeśli Agent sieciowy nie jest zainstalowany na urządzeniach, do których przypisujesz zadanie *Zdalna dezinstalacja aplikacji*.

Określ konto użytkownika, z poziomu którego zostanie uruchomiony instalator aplikacji. Kliknij przycisk **Dodaj**, wybierz **Konto**, a następnie określ poświadczenia konta użytkownika.

Możesz określić kilka kont użytkowników, na przykład, jeśli żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, dla których definiujesz zadanie. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

10. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

11. Kliknij przycisk **Zakończ**.

    Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

12. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

13. W oknie właściwości zadania określ ogólne ustawienia zadania.

14. Kliknij przycisk **Zapisz**.

15. Uruchom zadanie ręcznie lub poczekaj na jego uruchomienie zgodne z terminarzem określonym w ustawieniach zadania.

Po zakończeniu zadania zdalnej dezinstalacji, wybrana aplikacja zostanie usunięta z wybranych urządzeń.

Przywracanie poprzedniej wersji obiektu

Jeśli to konieczne, możesz wycofać zmiany wprowadzone w obiekcie. Na przykład, konieczne może być przywrócenie ustawień profilu z określonego dnia.

W celu wycofania zmian wprowadzonych w obiekcie:

1. W oknie właściwości obiektu otwórz zakładkę **Historia rewizji**.

2. Na liście rewizji obiektu wybierz rewizję, do której chcesz wycofać zmiany.

3. Kliknij przycisk **Wycofaj**.

4. Kliknij **OK**, aby potwierdzić działanie.

Obiekt zostanie wycofany do wybranej rewizji. Lista rewizji obiektu wyświetla wpis dotyczący podjętego działania. Opis rewizji wyświetla informacje o numerze rewizji, do której wycofałeś obiekt.

Operacja wycofywania jest dostępna tylko w przypadku obiektów zasad i zadań.

Zadania

Ta sekcja opisuje zadania używane przez Kaspersky Security Center.

Informacje o zadaniach

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

Zadania dla określonej aplikacji można utworzyć przy użyciu Kaspersky Security Center Web Console tylko wtedy, gdy wtyczka administracyjna dla tej aplikacji jest zainstalowana na serwerze Kaspersky Security Center Web Console Server.

Zadania mogą być wykonywane na Serwerze administracyjnym i na urządzeniach.

Zadania, które są wykonywane na Serwerze administracyjnym, obejmują:

- Automatyczne rozsyłanie raportów
- Pobieranie uaktualnień do repozytorium
- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Obsługa baz danych

Na urządzeniach wykonywane są następujące typy zadań:

- *Zadania lokalne*—zadania wykonywane na określonym urządzeniu

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

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

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

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

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

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

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

Wyniki wykonania zadań są zapisywane w dzienniku zdarzeń systemu operacyjnego na każdym urządzeniu, w dzienniku zdarzeń systemu operacyjnego na Serwerze administracyjnym, a także w bazie danych Serwera administracyjnego.

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

Informacje o obszarze zadania

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

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

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

- Ręcznie określ pewne urządzenia.

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

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

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

- Utwórz wybór urządzeń.

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

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

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

Tworzenie zadania

W celu utworzenia zadania:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z jego instrukcjami.
3. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
4. Kliknij przycisk **Zakończ**.

Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

Ręczne uruchamianie zadania

Aplikacja jest uruchamiana zgodnie z ustawieniami terminarza, określonymi we właściwościach każdego zadania. Możesz ręcznie uruchomić zadanie w dowolnym momencie.

W celu ręcznego uruchomienia zadania:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Na liście zadań zaznacz pole obok zadania, które chcesz uruchomić.
3. Kliknij przycisk **Uruchom**.

Zadanie zostanie uruchomione. Możesz sprawdzić stan zadania w kolumnie **Stan** lub klikając przycisk **Wynik**.

Przeglądanie listy zadań

Możesz przejrzeć listę zadań, które zostały utworzone w Kaspersky Security Center.

W celu przejrzenia listy zadań,

W menu głównym przejdź do **Urządzenia** → **Zadania**.

Zostanie wyświetlona lista zadań. Zadania są grupowane według nazw aplikacji, których dotyczą. Na przykład, zadanie Zdalna dezinstalacja aplikacji dotyczy Serwera administracyjnego, a zadanie Wyszukiwanie luk i wymaganych aktualizacji odnosi się do Agenta sieciowego.

W celu przejrzenia właściwości zadania:

Kliknij nazwę zadania.

Okno właściwości zadania zostanie wyświetlone z kilkoma nazwanymi zakładkami. Na przykład, **Typ zadania** jest wyświetlany na zakładce **Ogólne**, a terminarz zadania na zakładce **Terminarz**.

Ogólne ustawienia zadania

Ta sekcja zawiera ustawienia, które możesz przeglądać i konfigurować dla większości swoich zadań. Lista dostępnych ustawień zależy od konfigurowanego zadania.

Ustawienia określone podczas tworzenia zadania

Podczas tworzenia zadania możesz określić następujące ustawienia. Niektóre z tych ustawień mogą także zostać zmodyfikowane we właściwościach utworzonego zadania.

- Ustawienia ponownego uruchamiania systemu operacyjnego:
  - **Nie uruchamiaj ponownie urządzenia**

    Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

  - **Uruchom urządzenie ponownie**

    Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

  - **Pytaj użytkownika o akcję**

    Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

    Domyślnie opcja ta jest zaznaczona.

  - **Ponawiaj pytanie co (min)**

    Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

    Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

    Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

  - **Uruchom ponownie po (min)**

Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- Wymuś zamknięcie aplikacji dla zablokowanych sesji

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

- Ustawienia terminarza zadania:

  - **Ustawienia Zaplanowane uruchomienie**

    - Co N godzin

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

      Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

    - Co N dni

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

      Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

    - Co N tygodni

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

      Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

    - Co N minut

      Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

      Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Ręcznie**

  Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

  Domyślnie opcja ta jest włączona.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po pobraniu nowych aktualizacji do repozytorium**

  Zadanie jest uruchamiane po pobraniu uaktualnień do repozytorium. Na przykład, możesz użyć tego terminarza dla zadania wyszukiwania luk i wymaganych aktualizacji.

- **Po epidemii wirusa**

Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

- Ochrona antywirusowa stacji roboczych i serwerów plików
- Ochrona antywirusowa bram internetowych
- Ochrona antywirusowa serwerów pocztowych

Domyślnie, zaznaczone są wszystkie typy aplikacji.

Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest włączona.

- Używaj automatycznie losowego opóźnienia dla uruchamiania zadań

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

- Urządzenia, do których zadanie zostanie przypisane:
  - **Wybierz urządzenia sieciowe wykryte przez Serwer administracyjny**

    Zadanie jest przydzielane do określonych urządzeń. Określone urządzenia mogą obejmować urządzenia z grup administracyjnych oraz nieprzypisane urządzenia.

    Na przykład, możesz chcieć użyć tej opcji w zadaniu instalowania Agenta sieciowego na nieprzypisanych urządzeniach.

  - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

    Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

    Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

  - **Przypisz zadanie do wyboru urządzeń**

    Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

    Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

  - **Przypisz zadanie do grupy administracyjnej**

    Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

    Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

- Ustawienia konta:
  - **Konto domyślne**

    Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

    Domyślnie opcja ta jest zaznaczona.

  - **Określ konto**

Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

- **Konto**

  Konto, z poziomu którego zadanie jest uruchamiane.

- **Hasło**

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

Ustawienia określone po utworzeniu zadania

Następujące ustawienia możesz określić tylko po utworzeniu zadania.

- Ustawienia zadań grupowych:

  - **Roześlij do podgrup**

    Ta opcja jest dostępna tylko w ustawieniach zadań grupowych.

    Kiedy ta opcja jest włączona, zakres zadania obejmuje:

    - Grupa administracyjna, którą wybrano podczas tworzenia zadania.
    - Grupy administracyjne podporządkowane wybranej grupie administracyjnej na dowolnym poziomie niżej w hierarchii grup.

    Gdy ta opcja jest wyłączona, zakres zadania obejmuje tylko grupę administracyjną wybraną podczas tworzenia zadania.

    Domyślnie opcja ta jest włączona.

  - **Wyślij do podrzędnych i wirtualnych Serwerów administracyjnych**

    Gdy ta opcja jest włączona, zadanie działające na podstawowym serwerze administracyjnym jest również stosowane na pomocniczych (drugorzędnych) serwerach administracyjnych (w tym wirtualnych). Jeżeli zadanie tego samego typu już istnieje na pomocniczym serwerze administracyjnym, oba zadania są stosowane na pomocniczym serwerze administracyjnym — istniejące i odziedziczone z podstawowego serwera administracyjnego.

    Ta opcja jest dostępna tylko wtedy, gdy włączona jest opcja **Roześlij do podgrup**.

    Domyślnie opcja ta jest wyłączona.

- Zaawansowane ustawienia terminarza:

  - **Włącz urządzenia przed uruchomieniem zadania (min) przy użyciu funkcji Wake-on-LAN**

System operacyjny na urządzeniu zostanie uruchomiony o określonym czasie przed uruchomieniem zadania. Domyślnie czas ten wynosi pięć minut.

Włącz tę opcję, jeśli chcesz, aby zadanie było uruchamiane na wszystkich urządzeniach klienckich z obszaru zadania, w tym tych urządzeniach, które są wyłączone, gdy zadanie ma zostać uruchomione.

Jeśli chcesz, żeby urządzenie było automatycznie wyłączane po zakończeniu zadania, włącz opcję **Wyłącz urządzenia po zakończeniu zadania**. Ta opcja znajduje się w tym samym oknie.

Domyślnie opcja ta jest wyłączona.

- Wyłącz urządzenia po zakończeniu zadania

  Na przykład, możesz chcieć włączyć tę opcję dla zadania instalacji aktualizacji, które instaluje uaktualnienia na urządzeniach klienckich w każdy piątek w godzinach pracy, a następnie wyłącza te urządzenia w weekend.

  Domyślnie opcja ta jest wyłączona.

- Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż (min)

  Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

  Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

  Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.

- Ustawienia powiadomień:
  - Sekcja **Przechowywanie historii zadania**:
    - Przechowuj w bazie danych Serwera administracyjnego przez (dni)

      Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane na Serwerze administracyjnym przez określoną liczbę dni. Po upłynięciu tego okresu, informacje są usuwane z Serwera administracyjnego.

      Domyślnie opcja ta jest włączona.

    - Przechowuj w systemowym dzienniku zdarzeń urządzenia

      Zdarzenia aplikacji związane z wykonaniem zadania są przechowywane lokalnie w dzienniku zdarzeń systemu Windows każdego urządzenia klienckiego.

      Domyślnie opcja ta jest wyłączona.

    - Przechowuj w systemowym dzienniku zdarzeń Serwera administracyjnego

Zdarzenia aplikacji związane z wykonaniem zadania na wszystkich urządzeniach klienckich z obszaru zadania są przechowywane w sposób scentralizowany w dzienniku zdarzeń Windows systemu operacyjnego Serwera administracyjnego.

Domyślnie opcja ta jest wyłączona.

- **Zapisz wszystkie zdarzenia**

  Jeśli ta opcja jest zaznaczona, wszystkie zdarzenia dotyczące zadania zostaną zapisane w dziennikach zdarzeń.

- **Zapisz zdarzenia dotyczące postępu zadania**

  Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wykonania zadania zostaną zapisane w dziennikach zdarzeń.

- **Zapisz jedynie wyniki wykonywania zadania**

  Jeśli ta opcja jest zaznaczona, tylko zdarzenia dotyczące wyników zadania zostaną zapisane w dziennikach zdarzeń.

- **Powiadom administratora o wynikach wykonywania zadania**

  Możesz wybrać metody, przy użyciu których administratorzy otrzymają powiadomienia o wynikach wykonania zadań: za pośrednictwem poczty elektronicznej, przez SMS oraz poprzez uruchomienie pliku wykonywalnego. Aby skonfigurować powiadomienie, kliknij odnośnik **Ustawienia**.

  Domyślnie, wszystkie metody powiadamiania są wyłączone.

- **Powiadom tylko o błędach**

  Jeśli ta opcja jest włączona, administratorzy są powiadamiani tylko wtedy, gdy wykonanie zadania zakończy się błędem.

  Jeśli ta opcja jest wyłączona, administratorzy są powiadamiania po każdym zakończeniu wykonywania zadania.

  Domyślnie opcja ta jest włączona.

- Ustawienia zabezpieczeń.
- Ustawienia obszaru zadania.

  W zależności od sposobu określenia obszaru zadania, dostępne są następujące ustawienia:

  - **Urządzenia**

    Jeśli obszar zadania jest określany przez grupę administracyjną, możesz przejrzeć tę grupę. Nie ma tutaj dostępnych zmian. Jednakże możesz ustawić **Wykluczenia z zakresu zadania**.

    Jeśli obszar zadania jest określany przez listę urządzeń, możesz zmodyfikować tę listę poprzez dodanie i usunięcie urządzeń.

- **Wybór urządzeń**

  Możesz zmienić wybór urządzeń, do którego zadanie jest stosowane.

- **Wykluczenia z zakresu zadania**

  Możesz określić grupę urządzeń, do których zadanie nie jest stosowane. Grupy, które mają zostać wykluczone, mogą być tylko podgrupami grupami administracyjnej, do której zadanie jest stosowane.

- **Historia rewizji**.

Eksportowanie zadania

Kaspersky Security Center umożliwia zapisanie zadania i jego ustawień w pliku KLT. Możesz użyć tego pliku KLT do zaimportowania zapisanego zadania zarówno do Kaspersky Security Center Windows, jak i Kaspersky Security Center Linux.

W celu wyeksportowania zadania:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Zaznacz pole obok zadania, które chcesz wyeliminować.

   Nie można jednocześnie eksportować wielu zadań. Jeśli wybierzesz więcej niż jedno zadanie, przycisk **Eksportuj** będzie nieaktywny. Zadania Serwera administracyjnego i zadania lokalne są również niedostępne do eksportu.
3. Kliknij przycisk **Eksportuj**.
4. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę pliku zadania. Kliknij przycisk **Zapisz**.

   Okno **Zapisz jako** jest wyświetlane tylko wtedy, gdy korzystasz z przeglądarki Google Chrome, Microsoft Edge lub Opera. Jeśli używasz innej przeglądarki, plik zadania jest automatycznie zapisywany w folderze **Pobrane**.

Importowanie zadania

Kaspersky Security Center umożliwia import zadania z pliku KLT. Plik KLT zawiera wyeksportowane zadanie i jego ustawienia.

W celu zaimportowania zadania:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij przycisk **Importuj**.
3. Kliknij przycisk **Przeglądaj**, aby wybrać plik zadania, który chcesz zaimportować.
4. W otwartym oknie określ ścieżkę do pliku zadania KLT, a następnie kliknij przycisk **Otwórz**. Pamiętaj, że możesz wybrać tylko jeden plik zadania.

   Zadanie zostanie uruchomione.

5. Po pomyślnym przetworzeniu zadania wybierz urządzenia, do których chcesz przypisać zadanie. W tym celu wykonaj jedną z następujących czynności:

   - **Przypisz zadanie do grupy administracyjnej**

     Zadanie jest przypisywane do urządzeń znajdujących się w grupie administracyjnej. Możesz określić jedną z istniejących grup lub utworzyć nową grupę.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania wysyłania wiadomości do użytkowników, jeśli wiadomość jest specyficzna dla urządzeń znajdujących się w określonej grupie administracyjnej.

   - **Określ adresy urządzeń ręcznie lub zaimportuj adresy z listy**

     Możesz określić nazwy NetBIOS, nazwy DNS, adresy IP oraz podsieci IP urządzeń, do których chcesz przydzielić zadanie.

     Możesz użyć tej opcji do wykonania zadania dla określonej podsieci. Na przykład, możesz chcieć zainstalować pewną aplikację na urządzeniach księgowych lub przeskanować urządzenia w podsieci, która jest prawdopodobnie zainfekowana.

   - **Przypisz zadanie do wyboru urządzeń**

     Zadanie jest przypisywane do urządzeń znajdujących się w wyborze urządzeń. Możesz określić jeden z istniejących wyborów.

     Na przykład, możesz chcieć użyć tej opcji do uruchomienia zadania na urządzeniach z określoną wersją systemu operacyjnego.

6. Wybierz obszar zadania.

7. Kliknij przycisk **Zakończone**, aby zakończyć import zadania.

Pojawi się powiadomienie z wynikami importu. Jeśli zadanie zostało pomyślnie zaimportowane, możesz kliknąć łącze **Szczegóły**, aby wyświetlić właściwości zadania.

Po pomyślnym imporcie zadanie zostanie wyświetlone na liście zadań. Importowane są również ustawienia zadania i harmonogram. Zadanie zostanie uruchomione zgodnie z harmonogramem.

Jeśli nowo importowane zadanie ma identyczną nazwę jak istniejące zadanie, nazwa importowanego zadania jest rozszerzana o indeks **(<następny numer porządkowy>)**, na przykład: **(1)**, **(2)**.

Uruchamianie kreatora zmiany haseł w zadaniach

Dla zadania, które nie jest lokalne, możesz określić konto, z poziomu którego zadanie musi być uruchomione. Konto może zostać określone podczas tworzenia zadania lub we właściwościach istniejącego zadania. Jeśli określone konto jest używane zgodnie z instrukcjami bezpieczeństwa organizacji, te instrukcje mogą wymagać zmiany hasła do konta od czasu do czasu. Jeśli hasło do konta wygaśnie i ustawisz nowe, nie powiedzie się uruchomienie zadań, aż do momentu, gdy określisz nowe ważne hasło we właściwościach zadania.

Kreator zmiany haseł w zadaniach umożliwia automatyczne zastąpienie starego hasła nowym we wszystkich zadaniach, w których konto jest określone. Alternatywnie, możesz ręcznie zmienić to hasło we właściwościach każdego zadania.

W celu uruchomienia kreatora zmiany haseł w zadaniach:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Zarządzaj poświadczeniami kont do uruchamiania zadań**.

Postępuj zgodnie z instrukcjami kreatora.

Krok 1. Określanie danych uwierzytelniających

Określ nowe dane uwierzytelniające, które aktualnie są ważne w Twoim systemie (na przykład, w Active Directory). Jeśli przejdziesz do następnego kroku kreatora, Kaspersky Security Center sprawdzi, czy nazwa określonego konta odpowiada nazwie konta we właściwościach każdego zadania, które nie jest lokalne. Jeśli nazwy kont pasują do siebie, hasło we właściwościach zadania zostanie automatycznie zastąpione nowym.

W celu określenia nowego konta, wybierz opcję:

- **Użyj bieżącego konta**

  Kreator używa nazwy konta, na którym aktualnie zalogowano się do Kaspersky Security Center Web Console. Następnie ręcznie podaj hasło do konta w polu **Aktualne hasło do użycia w zadaniach**.

- **Określ inne konto**

  Określ nazwę konta, z poziomu którego zadania muszą być uruchamiane. Następnie określ hasło do konta w polu **Aktualne hasło do użycia w zadaniach**.

Jeśli uzupełnisz pole **Poprzednie hasło (opcjonalnie; jeśli chcesz zastąpić je obecnym)**, Kaspersky Security Center zastępuje hasło tylko dla tych zadań, w których zostanie wykryta nazwa konta oraz stare hasło. Zastępowanie odbywa się automatycznie. We wszystkich pozostałych przypadkach musisz wybrać działanie, jakie ma zostać podjęte w kolejnym kroku kreatora.

Krok 2. Wybieranie działania, jakie ma zostać podjęte

Jeśli nie określiłeś poprzedniego hasła w pierwszym kroku kreatora lub jeśli stare hasło nie odpowiada hasłom we właściwościach zadań, powinieneś wybrać działanie, jakie ma zostać wykonane na wykrytych zadaniach.

W celu wybrania akcji dla zadania:

1. Zaznacz pole obok zadania, dla której chcesz wybrać działanie.
2. Wykonaj jedną z następujących czynności:

   - Aby usunąć hasło we właściwościach zadania, kliknij **Usuń poświadczenia**.

     Zadanie zostanie przełączone do działania na koncie domyślnym.

- Aby zastąpić hasło nowym, kliknij **Wymuszaj zmianę hasła, nawet jeśli stare hasło jest niepoprawne lub nie zostało podane**.
- Aby anulować zmianę hasła, kliknij **Nie wybrano akcji**.

Wybrane akcje zostaną zastosowane po przejściu do następnego kroku kreatora.

Krok 3. Sprawdzanie wyników

W ostatnim kroku kreatora przejrzyj wyniki dla każdego wykrytego zadania. Aby zakończyć działanie kreatora, kliknij przycisk **Zakończ**.

Zarządzanie urządzeniami klienckimi

W tej sekcji można znaleźć opis sposobu zarządzania urządzeniami w grupach administracyjnych.

Ustawienia zarządzanego urządzenia

W celu sprawdzenia ustawień zarządzanego urządzenia:

1. Wybierz **Urządzenia** → **Zarządzane urządzenia**.
   Zostanie wyświetlona lista zarządzanych urządzeń.
2. Na liście zarządzanych urządzeń, kliknij odnośnik z nazwą żądanego urządzenia.

Zostanie wyświetlone okno właściwości wybranego urządzenia.

W górnej części okna właściwości wyświetlane są następujące zakładki reprezentujące główne grupy ustawień:

- Ogólne

Ta zakładka zawiera następujące sekcje:

- Sekcja **Ogólne** wyświetla ogólne informacje o urządzeniu klienckim. Informacje są dostarczane w oparciu o dane otrzymane podczas ostatniej synchronizacji urządzenia klienckiego z Serwerem administracyjnym:
  - Nazwa

    W tym polu możesz wyświetlić i zmodyfikować nazwę urządzenia klienckiego w grupie administracyjnej.
  - Opis

    W tym polu możesz wprowadzić dodatkowy opis urządzenia klienckiego.
  - Stan urządzenia

    Stan urządzenia klienckiego przypisany w oparciu o kryteria zdefiniowane przez administratora dla stanu ochrony antywirusowej na urządzeniu i aktywności urządzenia w sieci.
  - Pełna nazwa grupy

    Grupa administracyjna zawierająca urządzenie klienckie.
  - Ostatnia aktualizacja ochrony

    Data ostatniej aktualizacji antywirusowych baz danych lub aplikacji na urządzeniu.
  - Połączono z Serwerem administracyjnym

    Data i godzina ostatniego połączenia Agenta sieciowego, zainstalowanego na urządzeniu klienckim, z Serwerem administracyjnym.
  - Ostatnio dostępny

    Data i godzina, gdy urządzenie było ostatnio widoczne w sieci.
  - Wersja Agenta sieciowego

    Wersja zainstalowanego Agenta sieciowego.
  - Utworzono

    Data utworzenia urządzenia.
  - Właściciel urządzenia

Nazwa właściciela urządzenia. Możesz przypisać lub usunąć użytkownika jako właściciela urządzenia, klikając łącze **Zarządzaj właścicielem urządzenia**.

- Nie odłączaj od Serwera administracyjnego

  Jeśli ta opcja jest włączona, utrzymywana jest ciągła łączność pomiędzy zarządzanym urządzeniem a Serwerem administracyjnym. Możesz użyć tej opcji, jeśli nie używasz serwerów push, które zapewniają taką łączność.

  Jeśli ta opcja jest wyłączona, a serwery push nie są używane, zarządzane urządzenie będzie nawiązywało połączenie z Serwerem administracyjnym jedynie w celu synchronizacji danych lub przesłania informacji.

  Maksymalna całkowita liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego** to 300.

  Ta opcja jest wyłączona domyślnie na zarządzanych urządzeniach. Ta opcja jest włączona domyślnie na urządzeniu, na którym jest zainstalowany Serwer administracyjny i pozostaje włączona nawet w przypadku próby jej wyłączenia.

- Sekcja **Sieć** wyświetla następujące informacje o właściwościach sieci urządzenia klienckiego:
  - Adres IP

    Adres IP urządzenia.

  - Domena Windows

    Domena lub grupa robocza Windows, która zawiera urządzenie.

  - Nazwa DNS

    Nazwa domeny DNS urządzenia klienckiego.

  - Nazwa NetBIOS

    Nazwa urządzenia klienckiego w sieci Windows.

  - **Adres IPv6**: Adres IPv6 urządzenia klienckiego.
- Sekcja **System** zawiera informacje o systemie operacyjnym zainstalowanym na urządzeniu klienckim:
  - **System operacyjny**: Nazwa systemu operacyjnego urządzenia klienckiego.
  - **Architektura procesora**: Architektura procesora urządzenia klienckiego.
  - **Nazwa urządzenia**: Nazwa urządzenia klienckiego.
  - Typ maszyny wirtualnej

    Producent maszyny wirtualnej.

- **Dynamiczna maszyna wirtualna jako część VDI**

  Ten wiersz pokazuje, czy urządzenie klienckie jest dynamiczną maszyną wirtualną w ramach VDI.

- Sekcja **Ochrona** zawiera informacje o bieżącym stanie ochrony antywirusowej na urządzeniu klienckim:

  - **Widoczny**

    Stan widoczności urządzenia klienckiego.

  - **Stan urządzenia**

    Stan urządzenia klienckiego przypisany w oparciu o kryteria zdefiniowane przez administratora dla stanu ochrony antywirusowej na urządzeniu i aktywności urządzenia w sieci.

  - **Opis stanu**

    Stan ochrony urządzenia klienckiego i połączenia z Serwerem administracyjnym.

  - **Stan ochrony**

    To pole wyświetla bieżący stan ochrony urządzenia klienckiego w czasie rzeczywistym.

    Jeśli stan zmieni się na urządzeniu, nowy stan zostanie wyświetlony w oknie właściwości urządzenia dopiero po zsynchronizowaniu urządzenia klienckiego z Serwerem administracyjnym.

  - **Ostatnie pełne skanowanie**

    Data i godzina ostatniego skanowania w poszukiwaniu złośliwego oprogramowania przeprowadzonego na urządzeniu klienckim.

  - **Wykryto wirusa**

    Całkowita liczba zagrożeń wykrytych na urządzeniu klienckim od momentu zainstalowania aplikacji antywirusowej (pierwsze skanowanie) lub od momentu ostatniego zresetowania licznika zagrożeń.

  - **Obiekty, których leczenie nie powiodło się**

    Liczba nieprzetworzonych plików na urządzeniu klienckim.

    To pole ignoruje liczbę nieprzetworzonych plików na urządzeniach mobilnych.

  - **Stan szyfrowania dysku**

Bieżący stan szyfrowania plików na lokalnych dyskach urządzenia. Opis statusów znajduje się w pomocy Kaspersky Endpoint Security for Windows.

- Sekcja **Stan urządzenia zdefiniowany przez aplikację** zawiera informacje o stanie urządzenia zdefiniowanym przez zarządzaną aplikację zainstalowaną na urządzeniu. Ten stan urządzenia może różnić się od stanu zdefiniowanego przez Kaspersky Security Center.

- Aplikacje

  Ta zakładka zawiera listę wszystkich aplikacji firmy Kaspersky zainstalowanych na urządzeniu klienckim. Możesz kliknąć nazwę aplikacji, aby wyświetlić ogólne informacje o aplikacji, listę zdarzeń, które wystąpiły na urządzeniu oraz ustawienia aplikacji.

- Aktywne zasady i profile zasad

  Ta karta zawiera listę zasad i profili zasad, które są aktualnie aktywne na zarządzanym urządzeniu.

- Zadania

  W zakładce **Zadania** możesz zarządzać zadaniami urządzenia klienckiego: przeglądać listę istniejących zadań, tworzyć nowe zadania, usuwać, uruchamiać i zatrzymywać zadania, a także modyfikować ustawienia zadań i przeglądać wyniki ich wykonania. Lista zadań jest tworzona w oparciu o dane otrzymane w czasie ostatniej synchronizacji komputera klienckiego z Serwerem administracyjnym. Serwer administracyjny żąda od urządzenia klienckiego szczegółów dotyczących stanu zadania. Jeśli połączenie nie jest nawiązane, stan nie jest wyświetlany.

- Zdarzenia

  Zakładka **Zdarzenia** wyświetla zdarzenia zarejestrowane na Serwerze administracyjnym dla wybranego urządzenia klienckiego.

- Incydenty

  W zakładce **Incydenty** możesz przejrzeć, zmodyfikować i utworzyć zdarzenia dla urządzenia klienckiego. Zdarzenia mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora. Na przykład, jeśli niektórzy użytkownicy regularnie przenoszą szkodliwe programy ze swoich nośników wymiennych na urządzenia, administrator może utworzyć zdarzenie. W treści zdarzenia administrator może dostarczyć krótki opis zdarzenia oraz zalecane działania (na przykład działania dyscyplinarne wobec użytkownika), a także dodać odsyłacz.

  Zdarzenie, dla którego zostały wykonane wszystkie zalecane działania, nazywane jest *przetworzonym*. Obecność nieprzetworzonych zdarzeń może zostać wybrana jako warunek zmiany stanu urządzenia na *Krytyczny* lub *Ostrzeżenie*.

  Ta sekcja zawiera listę zdarzeń, które zostały utworzone dla urządzenia. Zdarzenia są klasyfikowane według priorytetu i typu. Typ zdarzenia jest definiowany przez aplikację Kaspersky, która utworzyła zdarzenie. Możesz podświetlić przetworzone zdarzenia na liście, zaznaczając pole w kolumnie **Przetworzone**.

- Znaczniki

W zakładce **Znaczniki** możesz zarządzać listą słów kluczowych, które są używane podczas wyszukiwania urządzeń klienckich: przejrzeć listę istniejących znaczników, przypisać znaczniki z listy, skonfigurować reguły automatycznego oznaczania oraz dodać nowe znaczniki i zmienić nazwy starszych znaczników, a także usunąć znaczniki.

- Zaawansowane

Ta zakładka zawiera następujące sekcje:

- **Rejestr aplikacji**. W tej sekcji możesz przejrzeć rejestr aplikacji zainstalowanych na urządzeniu klienckim i ich uaktualnień, a także możesz skonfigurować wyświetlanie rejestru aplikacji.

  Informacje o zainstalowanych aplikacjach są dostępne, jeśli Agent sieciowy zainstalowany na urządzeniu klienckim prześle żądane informacje do Serwera administracyjnego. Możesz skonfigurować przesyłanie informacji do Serwera administracyjnego w oknie właściwości Agenta sieciowego lub jego zasady, w sekcji **Repozytoria**. Informacje o zainstalowanych aplikacjach są dostarczane tylko dla urządzeń działających pod kontrolą systemu Windows.

  Agent sieciowy dostarcza informacje o aplikacjach w oparciu o dane pobrane z rejestru systemu.

  Kliknięcie nazwy aplikacji powoduje otwarcie okna zawierającego szczegółowe informacje o aplikacji oraz listę pakietów aktualizacji zainstalowanych dla aplikacji.

- **Pliki wykonywalne**. Ta sekcja wyświetla pliki wykonywalne wykryte na urządzeniu klienckim.

- **Punkty dystrybucji**. Ta sekcja zawiera listę punktów dystrybucji, z którymi urządzenie komunikuje się.

  - Eksportuj do pliku

    Kliknij przycisk **Eksportuj do pliku**, aby zapisać do pliku listę punktów dystrybucji, z którymi urządzenie komunikuje się. Domyślnie aplikacja eksportuje listę urządzeń do pliku CSV.

  - Właściwości

    Kliknij przycisk **Właściwości**, aby przejrzeć i skonfigurować punkt dystrybucji, z którym urządzenie komunikuje się.

- **Rejestr sprzętu**. W tej sekcji możesz wyświetlić informacje o sprzęcie zainstalowanym na urządzeniu klienckim.

- **Dostępne aktualizacje**. Sekcja ta wyświetla listę aktualizacji oprogramowania znajdujących się na tym urządzeniu, ale jeszcze nie zainstalowanych.

- **Luki w oprogramowaniu**. Ta sekcja zawiera informacje o lukach w aplikacjach firm trzecich zainstalowanych na urządzeniach klienckich.

  Aby zapisać luki w pliku, zaznacz pola wyboru obok luk, które chcesz zapisać, a następnie kliknij przycisk **Eksportuj wiersze do pliku CSV** lub przycisk **Eksportuj wiersze do pliku TXT**.

  Ta sekcja zawiera następujące ustawienia:

  - Pokaż tylko luki, które można naprawić

    Jeśli ta opcja jest włączona, sekcja wyświetla luki, które można naprawić przy użyciu poprawki.

    Jeśli ta opcja jest wyłączona, sekcja wyświetla luki, które można wyeliminować przy użyciu poprawki, oraz luki, dla których nie opublikowano poprawki.

    Domyślnie opcja ta jest włączona.

  - Właściwości luki

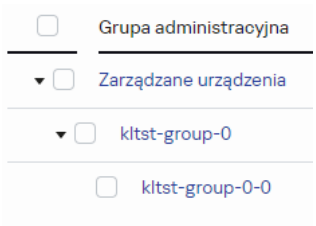
Na liście kliknij nazwę luki w oprogramowaniu, aby przejrzeć właściwości wybranej luki w oprogramowaniu w oddzielnym oknie. W oknie możesz wykonać następujące czynności:

- Zignoruj lukę w oprogramowaniu na tym zarządzanym urządzeniu (w Konsoli administracyjnej lub w konsoli Kaspersky Security Center Web Console).
- Przejrzyj listę zalecanych poprawek dla luki.
- Ręcznie określ aktualizacje oprogramowania, aby naprawić lukę (w Konsoli administracyjnej lub w Kaspersky Security Center Web Console).
- Przejrzyj instancje luki.
- Przejrzyj listę istniejących zadań, aby naprawić lukę i utworzyć nowe zadania w celu wyeliminowania luki.

- **Zdalna diagnostyka** W tej sekcji możesz przeprowadzić zdalną diagnostykę urządzeń klienckich.

Tworzenie grup administracyjnych

Od razu po zainstalowaniu Kaspersky Security Center, hierarchia grup administracyjnych zawiera tylko jedną grupę administracyjną, która nosi nazwę **Zarządzane urządzenia**. Podczas tworzenia hierarchii grup administracyjnych możesz dodać urządzenia, w tym maszyny wirtualne, do folderu **Zarządzane urządzenia**, a także możesz dodać zagnieżdżone grupy (patrz rysunek poniżej).



Wyświetlanie hierarchii grup administracyjnych

W celu utworzenia grupy administracyjnej:

1. W menu głównym przejdź do **Urządzenia** → **Hierarchia grup**.
2. W strukturze grupy administracyjnej wybierz grupę administracyjną, aby uwzględnić nową grupę administracyjną.
3. Kliknij przycisk **Dodaj**.
4. W oknie **Nazwa nowej grupy administracyjnej**, które zostanie otwarte, wprowadź nazwę grupy, a następnie kliknij przycisk **Dodaj**.

W nowej grupie administracyjnej z określoną nazwą pojawi się w hierarchii grup administracyjnych.

Aplikacja umożliwia tworzenie hierarchii grup administracyjnych opartej na strukturze Active Directory lub na strukturze sieci domeny. Strukturę grup możesz również utworzyć z pliku tekstowego.

W celu utworzenia struktury grup administracyjnych:

1. W menu głównym przejdź do **Urządzenia** → **Hierarchia grup**.
2. Kliknij przycisk **Importuj**.

Zostanie uruchomiony Kreator struktury nowej grupy administracyjnej. Postępuj zgodnie z instrukcjami kreatora.

Ręczne dodawanie urządzeń do grupy administracyjnej

Możesz automatycznie przenieść urządzenia do grup administracyjnych, tworząc reguły przenoszenia urządzeń, lub ręcznie, przenosząc urządzenia z jednej grupy administracyjnej do innej lub dodając urządzenia do wybranej grupy administracyjnej. Ta sekcja opisuje sposób ręcznego dodawania urządzeń do grupy administracyjnej.

W celu ręcznego dodania jednego lub kilku urządzeń do wybranej grupy administracyjnej:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.
2. Kliknij odnośnik **Obecna ścieżka:** `<obecna ścieżka>` nad listą.
3. W otwartym oknie wybierz grupę administracyjną, do której chcesz dodać urządzenia.
4. Kliknij przycisk **Dodaj urządzenia**.
   Zostanie uruchomiony Kreator przenoszenia urządzeń.
5. Utwórz listę urządzeń, które chcesz dodać do grupy administracyjnej.

   Możesz dodać tylko urządzenia, dla których informacje zostały już dodane do bazy danych Serwera administracyjnego przy podłączeniu urządzenia lub po wykrywaniu urządzeń.

   Wybierz sposób dodawania urządzeń do listy:

   - Kliknij przycisk **Dodaj urządzenia**, a następnie określ urządzenia w jeden z następujących sposobów:
     - Wybierz urządzenia z listy urządzeń wykrytych przez Serwer administracyjny.
     - Określ adres IP urządzenia lub zakres IP.
     - Określ nazwę NetBIOS lub nazwę DNS urządzenia.

       Pole nazwy urządzenia nie może zawierać spacji lub następujących zakazanych znaków: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %
   - Kliknij przycisk **Zaimportuj urządzenia z pliku**, aby zaimportować listę urządzeń z pliku .txt. Adres lub nazwa każdego urządzenia musi znajdować się w oddzielnym wierszu.

     Plik nie może zawierać spacji lub następujących zakazanych znaków: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %
6. Przejrzyj listę urządzeń, które mają zostać dodane do grupy administracyjnej. Możesz edytować listę, dodając lub usuwając urządzenia.

7. Jeśli upewnisz się, że lista jest poprawna, kliknij przycisk **Dalej**.

Kreator przetwarza listę urządzeń i wyświetla wynik. Pomyślnie przetworzone urządzenia zostaną dodane do grupy administracyjnej i będą wyświetlane na liście urządzeń pod nazwami wygenerowanymi przez Serwer administracyjny.

Ręczne przenoszenie urządzeń do grupy administracyjnej

Możesz przenieść urządzenia z jednej grupy administracyjnej do innej lub z grupy nieprzypisanych urządzeń do grupy administracyjnej.

W celu przeniesienia jednego lub kilku urządzeń do wybranej grupy administracyjnej:

1. Otwórz grupę administracyjną, z której chcesz przenieść urządzenia. W tym celu wykonaj jedną z następujących czynności:

   - Aby otworzyć grupę administracyjną, w menu głównym przejdź do **Urządzenia** → **Grupy** → **<group name>** → **Zarządzane urządzenia**.

   - Aby otworzyć grupę **Urządzenia nieprzypisane**, w menu głównym przejdź do **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane**.

2. Zaznacz pola obok urządzeń, które chcesz przenieść do innej grupy.

3. Kliknij przycisk **Przenieś do grupy**.

4. W hierarchii grup administracyjnej zaznacz pole obok grupy administracyjnej, do której chcesz przenieść wybrane urządzenia.

5. Kliknij przycisk **Przenieś**.

Wybrane urządzenia są przenoszone do wybranej grupy administracyjnej.

Tworzenie reguł przenoszenia urządzeń

Możesz skonfigurować reguły przenoszenia urządzeń, czyli reguły, które automatycznie przypisują urządzenia do grup administracyjnych.

W celu utworzenia reguły przenoszenia:

1. W menu głównym przejdź na **Urządzenia** → **Reguły przenoszenia**.

2. Kliknij **Dodaj**.

3. W otwartym oknie, na zakładce **Ogólne** określ następujące informacje:

   - **Nazwa reguły**

Wprowadź nazwę nowej reguły.

Jeśli kopiujesz regułę, nowa reguła otrzyma tę samą nazwę co reguła źródłowa, ale do nazwy zostanie dodany indeks w formacie (), na przykład: (1).

- **Grupa administracyjna**

  Wybierz grupę administracyjną, do której urządzenia są przenoszone automatycznie.

- **Zastosuj regułę**

  Możesz wybrać jedną z następujących opcji:

  - Uruchom raz dla każdego urządzenia.

    Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom.

  - Uruchom raz na każdym urządzeniu, a następnie po każdej instalacji Agenta sieciowego.

    Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom, a następnie tylko wtedy, gdy Agent sieciowy jest ponownie instalowany na tych urządzeniach.

  - Reguła stosowana cały czas.

    Reguła jest stosowana zgodnie z terminarzem, który Serwer administracyjny konfiguruje automatycznie (zazwyczaj co kilka godzin).

- **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**

  Jeśli ta opcja jest włączona, do wybranej grupy zostaną przeniesione tylko urządzenia nieprzypisane.

  Jeśli ta opcja jest wyłączona, urządzenia, które już należą do innych grup administracyjnych, a także urządzenia nieprzypisane, zostaną przeniesione do wybranej grupy.

- **Włącz regułę**

  Jeśli ta opcja jest włączona, reguła jest włączona i zaczyna działać po jej zapisaniu.

  Jeśli ta opcja jest wyłączona, reguła zostaje utworzona, ale nie jest włączona. Nie będzie działać, dopóki nie włączysz tej opcji.

4. Na karcie **Warunki reguły** określ co najmniej jedno kryterium, według którego urządzenia są przenoszone do grupy administracyjnej.
5. Kliknij **Zapisz**.

Reguła przenoszenia została utworzona. Jest wyświetlana na liście reguł przenoszenia.

Im wyższa pozycja na liście, tym wyższy priorytet reguły. Aby zwiększyć lub zmniejszyć priorytet reguły przenoszenia, przesuń regułę odpowiednio w górę lub w dół na liście za pomocą myszy.

Jeśli atrybuty urządzenia spełniają warunki kilku reguł, urządzenie zostanie przeniesione do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

Kopiowanie reguł przenoszenia urządzeń

Możesz kopiować reguły przenoszenia, na przykład, jeśli chcesz mieć kilka identycznych reguł dla różnych docelowych grup administracyjnych.

W celu skopiowania istniejącej reguły przenoszenia:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź na **Urządzenia** → **Reguły przenoszenia**.
   - W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Reguły przenoszenia**.

   Zostanie wyświetlona lista reguł przenoszenia.

2. Zaznacz pole obok reguły, którą chcesz skopiować.
3. Kliknij **Kopiuj**.
4. W otwartym oknie zmień następujące informacje na zakładce **Ogólne** lub nie wprowadzaj żadnych zmian, jeśli chcesz tylko skopiować regułę bez zmiany jej ustawień:

   - **Nazwa reguły**

     Wprowadź nazwę nowej reguły.

     Jeśli kopiujesz regułę, nowa reguła otrzyma tę samą nazwę co reguła źródłowa, ale do nazwy zostanie dodany indeks w formacie (), na przykład: (1).

   - **Grupa administracyjna**

     Wybierz grupę administracyjną, do której urządzenia są przenoszone automatycznie.

   - **Zastosuj regułę**

     Możesz wybrać jedną z następujących opcji:

     - Uruchom raz dla każdego urządzenia.

       Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom.

     - Uruchom raz na każdym urządzeniu, a następnie po każdej instalacji Agenta sieciowego.

       Reguła jest stosowana raz dla każdego urządzenia, które odpowiada Twoim kryteriom, a następnie tylko wtedy, gdy Agent sieciowy jest ponownie instalowany na tych urządzeniach.

     - Reguła stosowana cały czas.

       Reguła jest stosowana zgodnie z terminarzem, który Serwer administracyjny konfiguruje automatycznie (zazwyczaj co kilka godzin).

   - **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**

Jeśli ta opcja jest włączona, do wybranej grupy zostaną przeniesione tylko urządzenia nieprzypisane.

Jeśli ta opcja jest wyłączona, urządzenia, które już należą do innych grup administracyjnych, a także urządzenia nieprzypisane, zostaną przeniesione do wybranej grupy.

- **Włącz regułę**

  Jeśli ta opcja jest włączona, reguła jest włączona i zaczyna działać po jej zapisaniu.

  Jeśli ta opcja jest wyłączona, reguła zostaje utworzona, ale nie jest włączona. Nie będzie działać, dopóki nie włączysz tej opcji.

5. Na karcie **Warunki reguły** określ co najmniej jedno kryterium dla urządzeń, które mają być przenoszone automatycznie.
6. Kliknij **Zapisz**.

Nowa reguła przenoszenia została utworzona. Jest wyświetlana na liście reguł przenoszenia.

Warunki dla reguły przenoszenia urządzenia

Kiedy tworzysz lub kopiujesz regułę przenoszenia urządzeń klienckich do grup administracyjnych, na zakładce **Warunki reguły** ustawiasz warunki przenoszenia urządzeń . Aby określić, które urządzenia przenieść, możesz skorzystać z następujących kryteriów:

- Tagi przypisane do urządzeń klienckich.
- Parametry sieciowe. Na przykład możesz przenieść urządzenia z adresami IP z określonego zakresu.
- Aplikacje zarządzane zainstalowane na urządzeniach klienckich, na przykład Agent sieciowy lub Serwer administracyjny.
- Maszyny wirtualne, które są urządzeniami klienckimi.
- Informacje o jednostce organizacyjnej Active Directory (OU) z urządzeniami klienckimi.
- Informacje o segmencie chmury z urządzeniami klienckimi.

Poniżej znajdziesz opis, jak określić te informacje w regule przenoszenia urządzeń.

Jeśli określisz kilka warunków w regule, operator logiczny AND działa i wszystkie warunki mają zastosowanie w tym samym czasie. Jeśli nie zaznaczysz żadnych opcji lub pozostawisz niektóre pola puste, takie warunki nie mają zastosowania.

Zakładka Znaczniki

Na tej zakładce można skonfigurować regułę przenoszenia urządzeń na podstawie znaczników urządzenia, które zostały wcześniej dodane do opisów urządzeń klienckich. Aby to zrobić, wybierz wymagane tagi. Możesz także włączyć następujące opcje:

- **Zastosuj do urządzeń bez określonych znaczników**

Jeśli ta opcja jest włączona, wszystkie urządzenia z określonymi tagami są wykluczane z reguły przenoszenia urządzeń. Jeśli ta opcja jest wyłączona, reguła przenoszenia urządzeń dotyczy urządzeń ze wszystkimi wybranymi tagami.

Domyślnie opcja ta jest wyłączona.

- Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny

  Jeśli ta opcja jest włączona, reguła przenoszenia urządzeń dotyczy urządzeń klienckich z co najmniej jednym z wybranych tagów. Jeśli ta opcja jest wyłączona, reguła przenoszenia urządzeń dotyczy urządzeń ze wszystkimi wybranymi tagami.

  Domyślnie opcja ta jest wyłączona.

Karta Sieć

Na tej karcie możesz określić dane sieciowe urządzeń, które uwzględnia reguła przenoszenia urządzeń:

- Nazwa urządzenia w sieci Windows

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- Domena Windows

  Reguła przenoszenia urządzeń dotyczy wszystkich urządzeń zawartych w określonej domenie Windows.

- Nazwa DNS urządzenia

  Nazwa domeny DNS urządzenia klienckiego, które chcesz przenieść. Wypełnij to pole, jeśli Twoja sieć zawiera serwer DNS.

  Jeśli dla bazy danych używanej z Kaspersky Security Center ustawione jest sortowanie z rozróżnianiem wielkości liter, zachowaj wielkość liter podczas określania nazwy DNS urządzenia. W przeciwnym razie reguła przenoszenia urządzenia nie będzie działać.

- Domena DNS

  Reguła przenoszenia urządzeń dotyczy wszystkich urządzeń zawartych w określonym głównym sufiksie DNS. Wypełnij to pole, jeśli Twoja sieć zawiera serwer DNS.

- Zakres IP

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

- Adres IP do łączenia z Serwerem administracyjnym

Jeżeli ta opcja jest włączona, możesz ustawić adresy IP, za pomocą których urządzenia klienckie będą połączone z Serwerem administracyjnym. W tym celu określ zakres adresów IP, który zawiera wszystkie niezbędne adresy IP.

Domyślnie opcja ta jest wyłączona.

- Zmieniono profil połączenia

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich ze zmienionym profilem połączenia.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich, których profil połączenia nie uległ zmianie.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

- Zarządzane przez inny Serwer administracyjny

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez inne Serwery administracyjne. Te serwery różnią się od serwera, na którym konfigurujesz regułę przenoszenia urządzeń.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich zarządzanych przez bieżący Serwer administracyjny.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

Karta Aplikacje

Na tej karcie możesz skonfigurować regułę przenoszenia urządzeń na podstawie zarządzanych aplikacji i systemów operacyjnych zainstalowanych na urządzeniach klienckich:

- Agent sieciowy jest zainstalowany

  Wybierz jedną z następujących wartości:

  - **Tak**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich z zainstalowanym Agentem sieciowym.
  - **Nie**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń klienckich, na których nie jest zainstalowany Agent sieciowy.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

- Aplikacje

Określ, jakie zarządzane aplikacje powinny być zainstalowane na urządzeniach klienckich, aby reguła przenoszenia urządzeń miała zastosowanie do tych urządzeń. Na przykład możesz wybrać **Agent sieciowy Kaspersky Security Center 14.2** lub **Serwer administracyjny Kaspersky Security Center 14.2**.

Jeśli nie wybierzesz żadnej zarządzanej aplikacji, warunek nie ma zastosowania.

- Wersja systemu operacyjnego

  Urządzenia klienckie można usuwać na podstawie wersji systemu operacyjnego. W tym celu określ systemy operacyjne, które powinny być zainstalowane na urządzeniach klienckich. W rezultacie reguła przenoszenia urządzeń dotyczy urządzeń klienckich z wybranymi systemami operacyjnymi.

  Jeśli nie włączysz tej opcji, warunek nie ma zastosowania. Domyślnie opcja ta jest wyłączona.

- Typ systemu operacyjnego (bity)

  Urządzenia klienckie można usuwać według rozmiarów bitowych systemu operacyjnego. W polu **Typ systemu operacyjnego (bity)** możesz wybrać jedną z następujących wartości:

  - **Nieznany**
  - **x86**
  - **AMD64**
  - **IA64**

  Aby sprawdzić rozmiar bitowy systemu operacyjnego urządzeń klienckich:

  1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.
  2. Kliknij przycisk **Ustawienia kolumn** ( ) po prawej.
  3. Wybierz opcję **Typ systemu operacyjnego (bity)** , a następnie kliknij przycisk **Zapisz** .

     Następnie rozmiar bitowy systemu operacyjnego jest wyświetlany dla każdego zarządzanego urządzenia.

- Wersja dodatku Service Pack systemu operacyjnego

  W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- Certyfikat użytkownika

  Wybierz jedną z następujących wartości:

  - **Zainstalowano** Reguła przenoszenia urządzeń dotyczy tylko urządzeń mobilnych z certyfikatem mobilnym.
  - **Nie zainstalowano**. Reguła przenoszenia urządzeń dotyczy tylko urządzeń mobilnych bez certyfikatu mobilnego.
  - **Nie wybrano wartości**. Warunek nie ma zastosowania.

- Kompilacja systemu operacyjnego

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować regułę przenoszenia urządzeń dla wszystkich numerów kompilacji z wyjątkiem określonego.

- Numer wersji systemu operacyjnego

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer wydania. Możesz także skonfigurować regułę przenoszenia urządzeń dla wszystkich numerów wersji z wyjątkiem określonego.

Karta Maszyny wirtualne

Na tej karcie możesz skonfigurować regułę przenoszenia urządzeń w zależności od tego, czy urządzenia klienckie są maszynami wirtualnymi, czy częścią infrastruktury pulpitu wirtualnego (VDI):

- Jest maszyną wirtualną

  Z listy rozwijalnej możesz wybrać jedną z następujących opcji:
  - **N/D**. Warunek nie ma zastosowania.
  - **Nie**. Przenosi urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Przenosi urządzenia, które są maszynami wirtualnymi.

- **Typ maszyny wirtualnej**

- Część Virtual Desktop Infrastructure

  Z listy rozwijalnej możesz wybrać jedną z następujących opcji:
  - **N/D**. Warunek nie ma zastosowania.
  - **Nie**. Przenieś urządzenia, które nie są częścią VDI.
  - **Tak**. Przenieś urządzenia, które są częścią VDI.

Karta Active Directory

Na tej karcie możesz określić, że konieczne jest przeniesienie urządzeń znajdujących się w jednostce organizacyjnej Active Directory. Możesz także przenosić urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej Active Directory:

- Urządzenie znajduje się w jednostce organizacyjnej Active Directory

  Jeśli ta opcja jest włączona, reguła przenoszenia urządzeń dotyczy urządzeń z jednostki organizacyjnej Active Directory określonej na liście pod opcją.

  Domyślnie opcja ta jest wyłączona.

- Uwzględnij podrzędne jednostki organizacyjne

  Jeśli ta opcja jest włączona, wybór zawiera urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej Active Directory.

  Domyślnie opcja ta jest wyłączona.

- **Przenieś urządzenia z podrzędnych jednostek do odpowiednich podgrup**
- **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń**
- **Usuń podgrupy, które nie znajdują się w strukturze Active Directory**
- Urządzenie należy do grupy Active Directory

  Jeśli ta opcja jest włączona, reguła przenoszenia urządzeń dotyczy urządzeń z grupy Active Directory określonej na liście pod opcją.

  Domyślnie opcja ta jest wyłączona.

Zakładka Segmenty chmury

Na tej zakładce możesz określić, że konieczne jest przeniesienie urządzeń należących do określonych segmentów chmury:

- Urządzenie znajduje się w segmencie chmury

  Jeśli wybierzesz tę opcję, reguła przenoszenia urządzeń zostanie zastosowana do urządzeń klienckich należących do segmentu chmury. Możesz wybrać żądany segment chmury aż do podsieci na liście pod opcją.

  Domyślnie opcja ta jest wyłączona.

- Włączając obiekty potomne

  W przypadku wybrania tej opcji reguła przenoszenia urządzeń dotyczy nie tylko wybranego segmentu chmury, ale także obiektów podrzędnych tego segmentu.

  Domyślnie opcja ta jest wyłączona.

- **Przenieś urządzenia z obiektów zagnieżdżonych do odpowiednich podgrup**
- **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń**

- **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury**
- Urządzenie wykryte przy pomocy API

  Z listy rozwijalnej możesz wybrać, czy urządzenie jest wykrywane przez narzędzia API:

  - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.
  - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.
  - **Google Cloud.** Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku Google Cloud.
  - **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale nie może zostać wykryte przy użyciu API.
  - **Brak wartości**. Warunek nie ma zastosowania.

Przeglądanie i konfigurowanie działań, gdy urządzenia wykazują brak aktywności

Jeśli urządzenia klienckie w grupie są nieaktywne, możesz otrzymać informacje na ten temat. Możesz także automatycznie usuwać takie urządzenia.

W celu przejrzenia lub skonfigurowania działań, gdy urządzenia w grupie wykazują brak aktywności:

1. W menu głównym przejdź do **Urządzenia** → **Hierarchia grup**.
2. Kliknij nazwę żądanej grupy administracyjnej.

   Zostanie otwarte okno właściwości grupy administracyjnej.
3. W oknie właściwości przejdź na zakładkę **Ustawienia**.
4. W sekcji **Dziedziczenie** włącz lub wyłącz następujące opcje:

   - Dziedzicz z grupy nadrzędnej

     Ustawienia z tej sekcji są dziedziczone od grupy nadrzędnej, w której znajduje się urządzenie klienckie. Jeśli ta opcja jest włączona, ustawienia w sekcji **Aktywność urządzenia w sieci** nie mogą być modyfikowane.

     Ta opcja jest dostępna tylko wtedy, gdy grupa administracyjna posiada grupę nadrzędną.

     Domyślnie opcja ta jest włączona.

   - Wymuś dziedziczenie ustawień w grupach podrzędnych

Wartości ustawień zostaną rozesłane do grup potomnych, ale we właściwościach grup potomnych te ustawienia są zablokowane.

Domyślnie opcja ta jest wyłączona.

5. W sekcji **Aktywność urządzenia** włącz lub wyłącz następujące opcje:

- **Powiadom administratora, jeżeli urządzenie jest nieaktywne dłużej niż (dni)**

  Jeśli ta opcja jest włączona, administrator otrzyma powiadomienie o nieaktywnych urządzeniach. Możesz określić przedział czasu, po upływie którego tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od bardzo dawna**. Domyślny przedział czasu wynosi 7 dni.

  Domyślnie opcja ta jest włączona.

- **Usuń urządzenie z grupy, jeżeli było nieaktywne dłużej niż (dni)**

  Jeśli ta opcja jest włączona, możesz określić przedział czasu, po upływie którego urządzenie zostanie automatycznie usunięte z grupy. Domyślny przedział czasu wynosi 60 dni.

  Domyślnie opcja ta jest włączona.

6. Kliknij **Zapisz**.

Twoje zmiany zostaną zapisane i zastosowane.

Informacje o stanach urządzeń

Kaspersky Security Center przypisze stan do każdego zarządzanego urządzenia. Określony stan zależy od tego, czy spełnione są warunki zdefiniowane przez użytkownika. W niektórych przypadkach, podczas przypisywania stanu do urządzenia, Kaspersky Security Center bierze pod uwagę flagę widoczności urządzenia w sieci (patrz tabela poniżej). Jeśli Kaspersky Security Center nie znajdzie urządzenia w sieci w ciągu dwóch godzin, flaga widoczności urządzenia zostanie ustawiona na *Nie jest widoczne*.

Stany są następujące:

- *Krytyczny* lub *Krytyczny / Widoczne*
- *Ostrzeżenie* lub *Ostrzeżenie / Widoczne*
- *OK* lub *OK / Widoczne*

Poniższa tabela wyświetla domyślne warunki, które muszą być spełnione, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia, wraz ze wszystkimi możliwymi wartościami.

Warunki przypisania stanu do urządzenia

Warunek	Opis warunku	Dostępne wartości
Aplikacja zabezpieczająca nie jest zainstalowana	Agent sieciowy jest zainstalowany na urządzeniu, ale aplikacja zabezpieczająca nie jest zainstalowana.	• Przycisk przełącznika jest ustawiony w pozycji włączenia.

		• Przycisk przełącznika jest ustawiony w pozycji wyłączenia.
Wykryto zbyt wiele wirusów	Niektóre wirusy zostały wykryte na urządzeniu przez zadanie wykrywania wirusów, na przykład, zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* oraz liczba wykrytych wirusów przekraczają określoną wartość.	Większe niż 0.
Poziom ochrony w czasie rzeczywistym jest inny niż poziom zdefiniowany przez administratora	Urządzenie jest widoczne w sieci, ale poziom ochrony w czasie rzeczywistym różni się od poziomu ustawionego (w warunku) przez administratora dla stanu urządzenia.	• Zatrzymane. • Wstrzymane. • Uruchomione.
Skanowanie w poszukiwaniu złośliwego oprogramowania nie było wykonywane od dłuższego czasu	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* nie było uruchamiane w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego 7 dni temu lub wcześniej.	Więcej niż 1 dzień.
Bazy danych są nieaktualne	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale antywirusowe bazy danych nie były aktualizowane na tym urządzeniu w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego dzień wcześniej lub jeszcze wcześniej.	Więcej niż 1 dzień.
Niepołączony od dłuższego czasu	Agent sieciowy jest zainstalowany na urządzeniu, ale urządzenie nie było połączone z Serwerem administracyjnym w określonym przedziale czasu, ponieważ urządzenie było wyłączone.	Więcej niż 1 dzień.
Wykryto aktywne zagrożenia	Liczba nieprzetworzonych obiektów w folderze **Aktywne zagrożenia** przekracza określoną wartość.	Więcej niż 0 elementów.
Wymagane jest ponowne uruchomienie	Urządzenie jest widoczne w sieci, ale aplikacja wymaga ponownego uruchomienia urządzenia dłużej niż określony przedział czasu i z jednego z wybranych powodów.	Więcej niż 0 minut.
Zainstalowane są niekompatybilne aplikacje	Urządzenie jest widoczne w sieci, ale inwentaryzacja oprogramowania wykonywana poprzez Agenta sieciowego wykryła niekompatybilne aplikacje zainstalowane na urządzeniu.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto luki w	Urządzenie jest widoczne w sieci, a Agent sieciowy jest	• Krytyczny.

oprogramowaniu	zainstalowany na urządzeniu, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* wykryło luki z określonym priorytetem w aplikacjach zainstalowanych na urządzeniu.	• Wysoki. • Średni. • Ignoruj, jeśli luka nie może być naprawiona. • Ignoruj, jeśli aktualizacja jest przypisana do instalacji.
Licencja utraciła ważność	Urządzenie jest widoczne w sieci, ale licencja utraciła ważność.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Licencja wkrótce utraci ważność	Urządzenie jest widoczne w sieci, ale licencja utraci ważność na urządzeniu za mniej niż określona liczba dni.	Więcej niż 0 dni.
Wyszukiwanie aktualizacji Windows Update nie było przeprowadzane od dłuższego czasu	Urządzenie jest widoczne w sieci, ale zadanie *Wykonaj synchronizację Windows Update* nie było uruchamiane w zdefiniowanym przedziale czasu.	Więcej niż 1 dzień.
Nieprawidłowy stan szyfrowania	Agent sieciowy jest zainstalowany na urządzeniu, ale wynik szyfrowania urządzenia jest równy określonej wartości.	• Nie zgadza się z zasadą w wyniku odmowy użytkownika (tylko dla urządzeń zewnętrznych). • Nie zgadza się z zasadą w wyniku błędu. • Po zastosowaniu zasady wymagane jest ponowne uruchomienie.

		• Nie określono zasady szyfrowania. • Nieobsługiwany. • Po zastosowaniu zasady.
Ustawienia urządzenia mobilnego nie są zgodne z zasadą	Ustawienia urządzenia mobilnego są inne niż ustawienia, które zostały określone w zasadzie Kaspersky Endpoint Security for Android podczas sprawdzania reguł zgodności.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto nieprzetworzone incydenty	Nieprzetworzone zdarzenia zostały wykryte na urządzeniu. Zdarzenia mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Stan urządzenia zdefiniowany przez aplikację	Stan urządzenia jest definiowany przez zarządzaną aplikację.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Brakuje miejsca na dysku urządzenia	Wolnego miejsca na dysku jest mniej niż określona wartość lub urządzenie nie mogło zostać zsynchronizowane z Serwerem administracyjnym. Stan *Krytyczny* lub *Ostrzeżenie* zmieniło się na stan *OK*, gdy urządzenie zostało pomyślnie zsynchronizowane z Serwerem administracyjnym, a wolna przestrzeń na urządzeniu jest większa niż lub równa określonej wartości.	Więcej niż 0 MB.
Zarządzanie urządzeniem nie	Podczas wykrywania urządzeń, urządzenie zostało rozpoznane jako widoczne w sieci, ale więcej niż trzy próby synchronizacji z	• Przycisk przełącznika

jest możliwe	Serwerem administracyjnym nie powiodły się.	jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Ochrona jest wyłączona	Urządzenie jest widoczne w sieci, ale aplikacja zabezpieczająca na urządzeniu została wyłączona na dłużej niż określony przedział czasu.	Więcej niż 0 minut.
Aplikacja zabezpieczająca nie jest uruchomiona	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale nie jest uruchomiona.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.

Kaspersky Security Center umożliwia skonfigurowanie automatycznego przełączania stanu urządzenia w grupie administracyjnej, gdy spełnione są określone warunki. Jeśli określone warunki są spełnione, do urządzenia klienckiego zostanie przypisany jeden z następujących stanów: *Krytyczny* lub *Ostrzeżenie*. Jeśli określone warunki zostaną spełnione, urządzeniu klienckiemu zostanie przypisany stan *OK*.

Różne stany mogą odpowiadać różnym wartościom jednego warunku. Na przykład, domyślnie, jeśli warunek **Bazy danych są nieaktualne** posiada wartość **Ponad 3 dni**, do urządzenia klienckiego zostaje przypisany stan *Ostrzeżenie*; jeśli wartość to **Ponad 7 dni**, wówczas zostanie przypisany stan *Krytyczny*.

Jeśli aktualizujesz Kaspersky Security Center z poprzedniej wersji, wartości warunku **Bazy danych są nieaktualne** dla przypisania stanu do *Krytyczne* lub *Ostrzeżenie* nie zmienią się.

Jeśli Kaspersky Security Center przypisze stan do urządzenia, dla niektórych warunków (patrz kolumna Opis warunku) brana jest pod uwagę flaga widoczności. Na przykład, jeśli do zarządzanego urządzenia został przypisany stan *Krytyczny*, ponieważ spełniony był warunek Bazy danych są nieaktualne, a później flaga widoczności została ustawiona dla urządzenia, wówczas do urządzenia zostanie przypisany stan *OK*.

Konfigurowanie przełączania stanów urządzeń

Możesz zmienić warunki, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia.

W celu włączenia zmiany stanu urządzenia na Krytyczny:

1. Otwórz okno właściwości w jeden z następujących sposobów:

   - W folderze **Zasady**, w menu kontekstowym profilu Serwera administracyjnego wybierz **Właściwości**.

- Z menu kontekstowego grupy administracyjnej wybierz **Właściwości**.

2. W oknie **Właściwości**, które zostanie otwarte, w panelu **Sekcje** wybierz **Stan urządzenia**.
3. W sekcji **Ustaw stan Krytyczny, jeśli** zaznacz pole obok warunku na liście.

   Jednakże możesz zmienić ustawienia, które nie są zablokowane w profilu nadrzędnym.

4. Dla wybranego warunku ustaw żądaną wartość.

   Możesz ustawić wartości dla niektórych, ale nie wszystkich, warunków.

5. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Krytyczne*.

W celu włączenia zmiany stanu urządzenia na Ostrzeżenie:

1. Otwórz okno właściwości w jeden z następujących sposobów:
   - W folderze **Zasady**, w menu kontekstowym profilu Serwera administracyjnego wybierz **Właściwości**.
   - Z menu kontekstowego grupy administracyjnej wybierz **Właściwości**.
2. W oknie **Właściwości**, które zostanie otwarte, w panelu **Sekcje** wybierz **Stan urządzenia**.
3. W prawej części, w sekcji **Ustaw stan Ostrzeżenie, jeśli** zaznacz pole obok warunku na liście.

   Jednakże możesz zmienić ustawienia, które nie są zablokowane w profilu nadrzędnym.

4. Dla wybranego warunku ustaw żądaną wartość.

   Możesz ustawić wartości dla niektórych, ale nie wszystkich, warunków.

5. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Ostrzeżenie*.

Zdalne połączenie z pulpitem urządzenia klienckiego

Administrator może uzyskać zdalny dostęp do pulpitu urządzenia klienckiego poprzez Agenta sieciowego zainstalowanego na urządzeniu klienckim. Zdalne połączenie z urządzeniem poprzez Agenta sieciowego jest możliwe nawet wtedy, gdy porty TCP i UDP urządzenia klienckiego są zamknięte.

Po nawiązaniu połączenia z urządzeniem, administrator uzyskuje pełny dostęp do informacji przechowywanych na tym urządzeniu, dzięki czemu może zarządzać aplikacjami, które są na nim zainstalowane.

Zdalne połączenie musi być dozwolone w ustawieniach systemu operacyjnego docelowego zarządzanego urządzenia. Na przykład, w systemie Windows 10 ta opcja nazywa się **Zezwalaj na połączenia Pomocy zdalnej z tym komputerem** (tę opcję można znaleźć w **Panel sterowania** → **System i zabezpieczenia** → **System** → **Ustawienia zdalne**). Jeśli posiadasz licencję dla funkcji Zarządzanie lukami i poprawkami, możesz wymusić włączenie tej funkcji podczas nawiązywania połączenia z zarządzanym urządzeniem. Jeśli nie masz licencji, włącz tę opcję lokalnie na docelowym zarządzanym urządzeniu. Jeśli ta opcja jest wyłączona, nawiązanie zdalnego połączenia nie jest możliwe.

W celu nawiązania zdalnego połączenia z urządzeniem, musisz posiadać dwa narzędzia:

- Narzędzie Kaspersky o nazwie klsctunnel. To narzędzie musi być przechowywane na stacji roboczej administratora. Tego narzędzia używasz do tunelowania połączenia między urządzeniem klienckim a Serwerem administracyjnym.

  Kaspersky Security Center umożliwia tunelowanie połączeń TCP z Konsoli administracyjnej poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym urządzeniu. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na urządzeniu z zainstalowaną Konsolą administracyjną z portem TCP na zarządzanym urządzeniu—jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a urządzeniem docelowym.

  Tunelowanie połączenia pomiędzy zdalnym urządzeniem klienckim a Serwerem administracyjnym jest wymagane, gdy port używany do nawiązania połączenia z Serwerem administracyjnym nie jest dostępny na urządzeniu. Port może być niedostępny na urządzeniu w następujących przypadkach:

  - Zdalne urządzenie jest podłączone do sieci lokalnej, która wykorzystuje mechanizm NAT.
  - Zdalne urządzenie jest częścią sieci lokalnej Serwera administracyjnego, ale jego port jest zamknięty przez zaporę sieciową.

- Standardowy składnik systemu Microsoft Windows o nazwie Podłączanie pulpitu zdalnego. Połączenie ze zdalnym pulpitem jest nawiązywane przy użyciu standardowego narzędzia Windows o nazwie mstsc.exe zgodnie z ustawieniami narzędzia.

  Połączenie z bieżącą sesją zdalnego pulpitu użytkownika jest nawiązywane bez zgody użytkownika. Po nawiązaniu przez administratora połączenia z sesją, użytkownik urządzenia zostaje odłączony od sesji bez wcześniejszego powiadomienia.

W celu zdalnego połączenia z pulpitem urządzenia klienckiego:

1. W Konsoli administracyjnej opartej na MMC, w menu kontekstowym Serwera administracyjnego wybierz **Właściwości**.
2. W otwartym oknie właściwości Serwera administracyjnego przejdź do **Ustawienia połączenia z Serwerem administracyjnym** → **Porty połączenia**.
3. Upewnij się, że opcja **Otwórz port RDP dla Kaspersky Security Center Web Console** jest włączona.
4. W Kaspersky Security Center Web Console przejdź do **Urządzenia** → **Zarządzane urządzenia** → **Grupy**, a następnie wybierz grupę administracyjną, która zawiera urządzenie, do którego chcesz uzyskać dostęp.
5. Zaznacz pole obok nazwy urządzenia, do którego chcesz uzyskać dostęp.
6. Kliknij przycisk **Połącz przez Pulpit zdalny**.

   Zostanie otwarte okno Pulpit zdalny (tylko Windows).
7. Włącz opcję **Zezwól na połączenie ze zdalnym pulpitem na zarządzanym urządzeniu**. W tym przypadku połączenie zostanie nawiązane nawet wtedy, gdy zdalne połączenia są aktualnie zabronione w ustawieniach systemu operacyjnego na zarządzanym urządzeniu.

Ta opcja jest dostępna tylko wtedy, gdy posiadasz licencję dla funkcji Zarządzanie lukami i poprawkami.

8. Kliknij przycisk **Pobierz**, aby pobrać narzędzie klsctunnel.
9. Kliknij przycisk **Kopiuj do schowka**, aby skopiować tekst z pola tekstowego. Ten tekst to Duży obiekt binarny (BLOB), który zawiera ustawienia wymagane do nawiązania połączenia między Serwerem administracyjnym a zarządzanym urządzeniem.

   BLOB jest ważny przez 3 minuty. Jeśli wygasł, otwórz ponownie okno Pulpit zdalny (tylko Windows), aby wygenerować nowy BLOB.

10. Uruchom narzędzie klsctunnel.

    Zostanie otwarte okno narzędzia.

11. Wklej skopiowany tekst do pola tekstowego.
12. Jeśli korzystasz z serwera proxy, zaznacz pole **Użyj serwera proxy**, a następnie określ ustawienia połączenia z serwerem proxy.
13. Kliknij przycisk **Otwórz port**.

    Zostanie otwarte okno logowania Podłączanie pulpitu zdalnego.

14. Podaj dane uwierzytelniające konta, na którym jesteś aktualnie zalogowany do konsoli Kaspersky Security Center Web Console.
15. Kliknij przycisk **Połącz**.

Po nawiązaniu połączenia z urządzeniem, pulpit jest dostępny w oknie Podłączanie pulpitu zdalnego systemu Microsoft Windows.

Nawiązywanie połączenia z urządzeniami poprzez udostępnianie pulpitu Windows

Administrator może uzyskać zdalny dostęp do pulpitu urządzenia klienckiego poprzez Agenta sieciowego zainstalowanego na urządzeniu klienckim. Zdalne połączenie z urządzeniem poprzez Agenta sieciowego jest możliwe nawet wtedy, gdy porty TCP i UDP urządzenia klienckiego są zamknięte.

Administrator może połączyć się z istniejącą sesją na urządzeniu klienckim bez rozłączania użytkownika w tej sesji. W tym przypadku administrator i użytkownik sesji na urządzeniu klienckim współdzielą dostęp do pulpitu.

W celu nawiązania zdalnego połączenia z urządzeniem, musisz posiadać dwa narzędzia:

- Narzędzie Kaspersky o nazwie klsctunnel. To narzędzie musi być przechowywane na stacji roboczej administratora. Tego narzędzia używasz do tunelowania połączenia między urządzeniem klienckim a Serwerem administracyjnym.

  Kaspersky Security Center umożliwia tunelowanie połączeń TCP z Konsoli administracyjnej poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym urządzeniu. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na urządzeniu z zainstalowaną Konsolą administracyjną z portem TCP na zarządzanym urządzeniu—jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a urządzeniem docelowym.

Tunelowanie połączenia pomiędzy zdalnym urządzeniem klienckim a Serwerem administracyjnym jest wymagane, gdy port używany do nawiązania połączenia z Serwerem administracyjnym nie jest dostępny na urządzeniu. Port może być niedostępny na urządzeniu w następujących przypadkach:

- Zdalne urządzenie jest podłączone do sieci lokalnej, która wykorzystuje mechanizm NAT.
- Zdalne urządzenie jest częścią sieci lokalnej Serwera administracyjnego, ale jego port jest zamknięty przez zaporę sieciową.

- Udostępnianie pulpitu Windows. Podczas łączenia się z istniejącą sesją zdalnego pulpitu użytkownik sesji na urządzeniu otrzymuje od administratora żądanie dotyczące połączenia. W raportach utworzonych przez Kaspersky Security Center nie są zapisywane żadne informacje dotyczące zdalnych działań wykonywanych na urządzeniu ani wyniki tych działań.

  Administrator może skonfigurować audyt aktywności użytkownika na zdalnym urządzeniu klienckim. W trakcie audytu aplikacja zapisuje informacje o plikach na urządzeniu klienckim, który został otwarty i/lub zmodyfikowany przez administratora.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego poprzez udostępnianie pulpitu Windows muszą być spełnione następujące warunki:

- Na urządzeniu klienckim powinien być zainstalowany system operacyjny Microsoft Windows Vista lub nowszy system Windows.
- Na stacji roboczej administratora powinien być zainstalowany system operacyjny Microsoft Windows Vista lub nowszy. Typ systemu operacyjnego urządzenia, na którym znajduje się Serwer administracyjny nie nakłada żadnych ograniczeń na łączenie poprzez udostępnianie pulpitu Windows.

  Aby sprawdzić, czy funkcja udostępniania pulpitu Windows znajduje się w posiadanej przez Ciebie edycji systemu Windows, upewnij się, że klucz CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} znajduje się w rejestrze systemu Windows.
- System Microsoft Windows Vista lub nowszy jest zainstalowany na urządzeniu klienckim.
- Kaspersky Security Center korzysta z licencji dla Zarządzania lukami i poprawkami.

W celu nawiązania połączenia z pulpitem urządzenia klienckiego poprzez udostępnianie pulpitu Windows:

1. W Konsoli administracyjnej opartej na MMC, w menu kontekstowym Serwera administracyjnego wybierz **Właściwości**.
2. W otwartym oknie właściwości Serwera administracyjnego przejdź do **Ustawienia połączenia z Serwerem administracyjnym** → **Porty połączenia**.
3. Upewnij się, że opcja **Otwórz port RDP dla Kaspersky Security Center Web Console** jest włączona.
4. W Kaspersky Security Center Web Console przejdź do **Urządzenia** → **Zarządzane urządzenia** → **Grupy**, a następnie wybierz grupę administracyjną, która zawiera urządzenie, do którego chcesz uzyskać dostęp.
5. Zaznacz pole obok nazwy urządzenia, do którego chcesz uzyskać dostęp.
6. Kliknij przycisk **Udostępnianie pulpitu Windows**.

   Zostanie otwarty Kreator Udostępnianie pulpitu Windows.
7. Kliknij przycisk **Pobierz**, aby pobrać narzędzie klsctunnel i zaczekaj, aż proces pobierania zostanie zakończony.

   Jeśli już posiadasz narzędzie klsctunnel, pomiń ten krok.
8. Kliknij przycisk **Dalej**.

9. Wybierz sesję na urządzeniu, z którym chcesz nawiązać połączenie, a następnie kliknij przycisk **Dalej**.

10. Na urządzeniu docelowym, w otwartym oknie dialogowym użytkownik musi zezwolić na sesję udostępniania pulpitu. W przeciwnym razie sesja nie będzie możliwa.

    Jeśli użytkownik urządzenia potwierdzi sesję udostępniania pulpitu, zostanie otwarta następna strona kreatora.

11. Kliknij przycisk **Kopiuj do schowka**, aby skopiować tekst z pola tekstowego. Ten tekst to Duży obiekt binarny (BLOB), który zawiera ustawienia wymagane do nawiązania połączenia między Serwerem administracyjnym a zarządzanym urządzeniem.

    BLOB jest ważny przez 3 minuty. Jeśli wygasł, wygeneruj nowy BLOB.

12. Uruchom narzędzie klsctunnel.

    Zostanie otwarte okno narzędzia.

13. Wklej skopiowany tekst do pola tekstowego.

14. Jeśli korzystasz z serwera proxy, zaznacz pole **Użyj serwera proxy**, a następnie określ ustawienia połączenia z serwerem proxy.

15. Kliknij przycisk **Otwórz port**.

Udostępnianie pulpitu rozpocznie się w nowym oknie. Jeśli chcesz wejść w interakcję z urządzeniem, kliknij ikonę menu ( ) w lewym górnym rogu okna, a następnie wybierz **Tryb interaktywny**.

Wybory urządzeń

Wybory urządzeń to narzędzie do filtrowania urządzeń zgodnie z określonymi warunkami. Możesz użyć wyborów urządzeń do zarządzania kilkoma urządzeniami: na przykład, aby przejrzeć raport dotyczący tylko tych urządzeń lub żeby przenieść wszystkie te urządzenia do innej grupy.

Kaspersky Security Center oferuje szeroki zakres *predefiniowanych wyborów* (na przykład: **Urządzenia ze stanem Krytyczny**, **Ochrona jest wyłączona**, **Wykryto aktywne zagrożenia**). Predefiniowanych wyborów nie można usunąć. Możesz także utworzyć i skonfigurować dodatkowe *wybory zdefiniowane przez użytkownika*.

W wyborach zdefiniowanych przez użytkownika możesz określić obszar wyszukiwania i wybrać wszystkie urządzenia, zarządzane urządzenia lub urządzenia nieprzypisane. Parametry wyszukiwania są określone w warunkach. W wyborze urządzeń możesz utworzyć kilka warunków z różnymi parametrami wyszukiwania. Na przykład, możesz utworzyć dwa warunki i określić różne zakresy IP w każdym z nich. Jeśli określono kilka warunków, wybór wyświetli urządzenia, które spełniają jakikolwiek warunek. Natomiast parametry wyszukiwania w obrębie warunku nakładają się na siebie. Jeśli zakres IP oraz nazwa zainstalowanej aplikacji są określone w warunku, wyświetlane będą tylko te urządzenia, na których jest zainstalowana aplikacja, a adres IP należy do określonego zakresu.

W celu wyświetlenia wyboru urządzeń:

1. Wykonaj jedną z poniższych czynności:

   - W menu głównym przejdź do **Urządzenia** → **Wybory urządzeń**.
   - W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wybory urządzeń**.

2. Na liście wyboru kliknij nazwę odpowiedniego wyboru.

Zostanie wyświetlony wynik wyboru urządzeń.

Tworzenie kryteriów wyboru urządzeń

W celu utworzenia kryterium wyboru urządzeń:

1. W menu głównym przejdź do **Urządzenia → Wybory urządzeń**.
   Zostanie wyświetlona lista wyborów urządzeń.
2. Kliknij przycisk **Dodaj**.
   Zostanie otwarte okno **Ustawienia wyboru urządzeń**.
3. Wprowadź nazwę nowego wyboru.
4. Określ typ urządzeń, które chcesz uwzględnić w wyborze urządzeń.
5. Kliknij przycisk **Dodaj**.
6. W oknie, które zostanie otwarte, określ warunki, które muszą być spełnione, aby uwzględnić urządzenia w tym wyborze, a następnie kliknij przycisk **OK**.
7. Kliknij przycisk **Zapisz**.

Wybór urządzeń zostanie utworzony i dodany do listy wyborów urządzeń.

Konfigurowanie kryteriów wyboru urządzeń

W celu skonfigurowania kryteriów wyboru urządzeń:

1. W menu głównym przejdź do **Urządzenia → Wybory urządzeń**.
   Zostanie wyświetlona lista wyborów urządzeń.
2. Wybierz odpowiednie urządzenie zdefiniowane przez użytkownika i kliknij przycisk **Właściwości**.
   Zostanie otwarte okno **Ustawienia wyboru urządzeń**.
3. Na karcie **Ogólne** kliknij łącze **Nowy warunek**.
4. Określ warunki, jakie muszą zostać spełnione do uwzględnienia urządzeń w tym wyborze.
5. Kliknij przycisk **Zapisz**.

Ustawienia zostaną zastosowane i zapisane.

Poniżej znajdują się opisy warunków przydzielania urządzeń do wyboru. Warunki są łączone przy użyciu operatora logicznego LUB: Wybór będzie zawierał urządzenia odpowiadające przynajmniej jednemu z wymienionych warunków.

Ogólny

W sekcji **Ogólny** możesz zmienić nazwę warunku wyboru oraz określić, czy ten warunek ma być odwrócony:

Odwróć warunek wyboru

Jeśli ta opcja jest włączona, określony warunek wyboru zostanie odwrócony. Wybór będzie zawierał wszystkie urządzenia, które nie spełniają warunku.

Domyślnie opcja ta jest wyłączona.

Sieć

W sekcji **Sieć** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich danymi sieciowymi:

- **Nazwa urządzenia lub adres IP**

  Nazwa sieciowa systemu Windows (nazwa NetBIOS) urządzenia lub adres IPv4 lub IPv6.

- **Domena Windows**

  Wyświetla wszystkie urządzenia znajdujące się w określonej domenie Windows.

- **Grupa administracyjna**

  Wyświetla urządzenia znajdujące się w określonej grupie administracyjnej.

- **Opis**

Tekst wyświetlany w oknie właściwości urządzenia: pole **Opis** sekcji **Ogólny**.

W celu opisania tekstu w polu **Opis** możesz użyć następujących znaków:

- W słowie:
  - *****. Zastępuje dowolny wiersz dowolną liczbą znaków.

    Na przykład:

    Aby opisać słowa **Serwer** lub **Serwera**, możesz wpisać **Serwer***.
  - **?.** Zastępuje dowolny pojedynczy znak.

    Na przykład:

    Aby opisać słowa **Okno** lub **Okna**, możesz wpisać **Okn?**.

    Gwiazdka (*****) lub znak zapytania (**?**) nie mogą być używane jako pierwsze symbole wyszukiwanego słowa.
- W celu wyszukania kilku słów użyj:
  - Spacji. Wyświetla wszystkie urządzenia, których opisy zawierają dowolne z wymienionych słów.

    Na przykład:

    Aby odszukać frazę zawierającą słowa **Podrzędny** lub **Wirtualny**, wprowadź **Podrzędny Wirtualny** w tekście wyszukiwania.
  - **+**. Jeśli przed wyrazem wpisano znak "+", wszystkie wyniki wyszukiwania będą zawierać ten wyraz.

    Na przykład:

    Aby odszukać frazę zawierającą zarówno **Podrzędny**, jak i **Wirtualny**, wprowadź **+Podrzędny+Wirtualny**.
  - **-**. Jeśli przed wyrazem wpisano znak "-", żaden z wyników wyszukiwania nie będzie zawierać tego wyrazu.

    Na przykład:

    Aby odszukać frazę zawierającą **Podrzędny** i nie zawierającą **Wirtualny**, wprowadź **+Podrzędny-Wirtualny**.
  - **"<jakikolwiek tekst>"**. Tekst w cudzysłowach musi znajdować się w tekście.

    Na przykład:

    Aby odszukać frazę zawierającą kombinację słów **Podrzędny Serwer**, wprowadź **„Podrzędny Serwer"** w tekście wyszukiwania.

- Zakres IP

  Jeśli ta opcja jest włączona, możesz wprowadzić początkowy i końcowy adres IP z zakresu adresów IP, do którego muszą zostać włączone odpowiednie urządzenia.

  Domyślnie opcja ta jest wyłączona.

Znaczniki

W sekcji **Znaczniki** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o słowa kluczowe (znaczniki), które wcześniej zostały dodane do opisów zarządzanych urządzeń:

- **Zastosuj, jeśli co najmniej jeden określony znacznik jest zgodny**

  Jeśli ta opcja jest włączona, w wynikach wyszukiwania będą wyświetlane urządzenia z opisami, które zawierają przynajmniej jeden z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, w wynikach wyszukiwania będą wyświetlane tylko urządzeni z opisami, które zawierają wszystkie wybrane znaczniki.

  Domyślnie opcja ta jest wyłączona.

- **Musi zawierać znacznik**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy zawierają wybrany znacznik. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

  Domyślnie opcja ta jest zaznaczona.

- **Nie może zawierać znacznika**

  Jeśli ta opcja jest zaznaczona, w wynikach wyszukiwania będą wyświetlane urządzenia, których opisy nie zawierają wybranego znacznika. Aby odszukać urządzenia, możesz użyć gwiazdki, która oznacza dowolny wiersz z dowolną liczbą znaków.

Active Directory

W sekcji **Active Directory** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich dane Active Directory:

- **Urządzenie znajduje się w jednostce organizacyjnej Active Directory**

  Jeśli ta opcja jest włączona, wybór będzie zawierał urządzenia z jednostki Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

- **Uwzględnij podrzędne jednostki organizacyjne**

  Jeśli ta opcja jest włączona, wybór zawiera urządzenia ze wszystkich podrzędnych jednostek organizacyjnych określonej jednostki organizacyjnej Active Directory.

  Domyślnie opcja ta jest wyłączona.

- **Urządzenie należy do grupy Active Directory**

  Jeśli ta opcja jest włączona, wybór będzie zawierał komputery z grupy Active Directory określonej w polu wejściowym.

  Domyślnie opcja ta jest wyłączona.

Aktywność sieciowa

W sekcji **Aktywność sieciowa** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich aktywnością sieciową:

- Urządzenie jest punktem dystrybucji

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:
  - **Tak**. Wybór zawiera urządzenia pełniące role punktów dystrybucji.
  - **Nie**. Urządzenia pełniące role punktów dystrybucji nie będą uwzględniane w wyborze.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Nie odłączaj od Serwera administracyjnego

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:
  - **Włączono**. Wybór będzie zawierał urządzenia, na których zaznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Wyłączono**. Wybór będzie zawierał urządzenia, na których odznaczono pole **Nie odłączaj od Serwera administracyjnego**.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Przełączanie profilu połączenia

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:
  - **Tak**. Wybór będzie zawierał urządzenia, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie**. Wybór nie będzie zawierał urządzeń, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Ostatnie połączenie z Serwerem administracyjnym

  To pole ustawia kryterium wyszukiwania urządzeń według godziny ostatniego połączenia z Serwerem administracyjnym.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego zostało nawiązane ostatnie połączenie pomiędzy Agentem sieciowym zainstalowanym na urządzeniu klienckim a Serwerem administracyjnym. Wybór będzie zawierał urządzenia mieszczące się w określonym przedziale czasu.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- Nowe urządzenia odnalezione podczas skanowania sieci

Wyszukiwanie nowych urządzeń, które zostały wykryte podczas przeszukiwania sieci w przeciągu kilku ostatnich dni.

Jeśli ta opcja jest włączona, wybór będzie zawierał nowe urządzenia wykryte podczas wykrywania urządzeń w czasie określonym w polu **Okres wykrywania (dni)**.

Jeśli ta opcja jest wyłączona, wybór będzie zawierał wszystkie urządzenia wykryte podczas wykrywania urządzeń.

Domyślnie opcja ta jest wyłączona.

- Dostępność urządzenia

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie widoczne w sieci.
  - **Nie**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie niewidoczne w sieci.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

Aplikacja

W sekcji **Aplikacja** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o wybraną zarządzaną aplikację:

- Nazwa aplikacji

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji Kaspersky.

  Lista zawiera tylko nazwy aplikacji z wtyczkami administracyjnymi zainstalowanych na stacji roboczej administratora.

  Jeśli żadna aplikacja nie została wybrana, kryterium nie będzie stosowane.

- Wersja aplikacji

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według numeru wersji aplikacji Kaspersky.

  Jeśli żaden numer wersji nie został określony, kryterium nie będzie stosowane.

- Nazwa aktualizacji krytycznej

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji lub numeru pakietu aktualizacyjnego.

  Jeśli pole będzie puste, kryterium nie będzie stosowane.

- Ostatnia aktualizacja modułów

Ta opcja może zostać użyta do ustawienia kryterium wyszukiwania urządzeń według godziny ostatniej aktualizacji modułów aplikacji zainstalowanych na tych urządzeniach.

Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego została wykonana ostatnia aktualizacja modułów aplikacji zainstalowanych na tych urządzeniach.

Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

Domyślnie pole to nie jest zaznaczone.

- Urządzenie jest zarządzane przez Kaspersky Security Center

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić urządzenia zarządzane poprzez Kaspersky Security Center:

  - **Tak**. Aplikacja uwzględni w wyborze urządzenia zarządzane poprzez Kaspersky Security Center.
  - **Nie**. Aplikacja uwzględni w wyborze urządzenia, jeśli nie są one zarządzane przez Kaspersky Security Center.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Aplikacja zabezpieczająca jest zainstalowana

  Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą:

  - **Tak**. Aplikacja uwzględni w wyborze wszystkie urządzenia z zainstalowaną aplikacją zabezpieczającą.
  - **Nie**. Aplikacja uwzględni w wyborze wszystkie urządzenia bez zainstalowanej aplikacji zabezpieczającej.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

System operacyjny

W sekcji **System operacyjny** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z typem systemu operacyjnego.

- Wersja systemu operacyjnego

  Jeśli pole jest zaznaczone, możesz wybrać system operacyjny z listy. Urządzenia, na których zainstalowany jest określony system operacyjny, są uwzględniane w wynikach wyszukiwania.

- Typ systemu operacyjnego (bity)

  Z listy rozwijalnej możesz wybrać architekturę swojego systemu operacyjnego, która określi sposób stosowania reguły przenoszenia do urządzenia (**Nieznany**, **x86**, **AMD64**, or **IA64**). Domyślnie, na liście nie wybrano żadnej opcji i tym samym nie zdefiniowano architektury systemu operacyjnego.

- Wersja dodatku Service Pack systemu operacyjnego

W tym polu możesz określić wersję pakietu systemu operacyjnego (w formacie *X.Y*), która będzie określać sposób stosowania reguły przenoszenia do urządzenia. Domyślnie nie jest zdefiniowana żadna wartość.

- Kompilacja systemu operacyjnego

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Numer kompilacji systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy numer kompilacji. Możesz także skonfigurować wyszukiwanie wszystkich numerów kompilacji, za wyjątkiem określonego.

- ID wersji systemu operacyjnego

  To ustawienie jest stosowane tylko w systemach operacyjnych Windows.

  Identyfikator wydania systemu operacyjnego. Możesz określić, czy wybrany system operacyjny musi mieć równy, wcześniejszy lub późniejszy identyfikator wydania. Możesz także skonfigurować wyszukiwanie wszystkich numerów identyfikatorów wydania, za wyjątkiem określonego.

Stan urządzenia

W sekcji **Stan urządzenia** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o opis stanu urządzeń z zarządzanej aplikacji:

- Stan urządzenia

  Lista rozwijalna, z której możesz wybrać jeden ze stanów urządzenia: *OK*, *Krytyczny*, or *Ostrzeżenie*.

- Opis stanu urządzenia

  W tym polu możesz zaznaczyć pola obok warunków, które, jeśli są spełnione, spowodują przypisanie do urządzenia jednego z następujących stanów: *OK, Krytyczny*, or *Ostrzeżenie*.

- Stan urządzenia zdefiniowany przez aplikację

  Lista rozwijalna, z której możesz wybrać stan ochrony w czasie rzeczywistym. Urządzenia z określonymi stanami ochrony w czasie rzeczywistym są uwzględniane w wyborze.

Składniki ochrony

W sekcji **Składniki ochrony** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich stan ochrony:

- Data opublikowania baz danych

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według daty opublikowania antywirusowej bazy danych. W polach do wprowadzania danych możesz określić przedział czasu, na podstawie którego wykonywane jest wyszukiwanie.

  Domyślnie opcja ta jest wyłączona.

- Licznik wpisów w bazie danych

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wpisów w bazie danych. W polach wejściowych możesz określić niższe i wyższe wartości progowe wpisów w antywirusowej bazie danych.

  Domyślnie opcja ta jest wyłączona.

- Ostatnie skanowanie

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według czasu ostatniego skanowania w poszukiwaniu złośliwego oprogramowania. W polach wejściowych możesz określić przedział czasu, w trakcie którego zostało wykonane ostatnie skanowanie w poszukiwaniu złośliwego oprogramowania.

  Domyślnie opcja ta jest wyłączona.

- Całkowita liczba wykrytych zagrożeń

  Jeśli ta opcja jest włączona, możesz wyszukiwać urządzenia klienckie według liczby wykrytych wirusów. W polach wejściowych możesz określić niższe i wyższe wartości progowe liczby wykrytych wirusów.

  Domyślnie opcja ta jest wyłączona.

Rejestr aplikacji

W sekcji **Rejestr aplikacji** możesz skonfigurować kryteria wyszukiwania urządzeń na podstawie aplikacji na nich zainstalowanych:

- Nazwa aplikacji

  Lista rozwijalna, z której możesz wybrać aplikację. Urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- Wersja aplikacji

  Pole, w którym możesz określić wersję wybranej aplikacji.

- Producent

  Lista rozwijalna, z której możesz wybrać producenta aplikacji zainstalowanej na urządzeniu.

- Stan aplikacji

Lista rozwijalna, z której możesz wybrać stan aplikacji (*Zainstalowana*, *Nie zainstalowana*). Urządzenia, na których określona aplikacja została zainstalowana lub nie została zainstalowana, w zależności od wybranego stanu, zostaną uwzględnione w wyborze.

- **Wyszukaj według aktualizacji**

  Jeśli ta opcja jest włączona, wyszukiwanie będzie się odbywać z użyciem szczegółów aktualizacji dla aplikacji zainstalowanych na odpowiednich urządzeniach. Po zaznaczeniu pola, pola **Nazwa aplikacji**, **Wersja aplikacji** i **Stan aplikacji** zostaną zmienione na **Nazwa aktualizacji**, **Wersja aktualizacji** i **Stan**.

  Domyślnie opcja ta jest wyłączona.

- **Nazwa niekompatybilnej aplikacji zabezpieczającej**

  Lista rozwijalna, z której możesz wybrać aplikacje zabezpieczające firm trzecich. Podczas wyszukiwania, urządzenia, na których jest zainstalowana określona aplikacja, są uwzględnione w wyborze.

- **Znacznik aplikacji**

  Z listy rozwijalnej możesz wybrać znacznik aplikacji. Wszystkie urządzenia, na których są zainstalowane aplikacje z wybranym znacznikiem w opisie, zostają uwzględnione w wyborze urządzeń.

- **Zastosuj do urządzeń bez określonych znaczników**

  Jeśli ta opcja jest włączona, wybór obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników.

  Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

  Domyślnie opcja ta jest wyłączona.

Rejestr sprzętu

W sekcji **Rejestr sprzętu** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o sprzęt na nich zainstalowany:

- **Urządzenie**

  Z listy rozwijalnej możesz wybrać typ jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent**

  Z listy rozwijalnej możesz wybrać nazwę producenta jednostki. Wszystkie urządzenia z tą jednostką zostają uwzględnione w wynikach wyszukiwania.

  Pole obsługuje wyszukiwanie pełnotekstowe.

- **Nazwa urządzenia**

Nazwa urządzenia w sieci Windows. Urządzenie z określoną nazwą zostanie uwzględniony w wyborze.

- **Opis**

  Opis urządzenia lub sprzętu. Urządzenia z opisem określonym w tym polu zostaną uwzględnione w wyborze.

  Opis urządzenia w dowolnym formacie może zostać wprowadzony w oknie właściwości tego urządzenia. Pole obsługuje wyszukiwanie pełnotekstowe.

- **Producent urządzenia**

  Nazwa producenta urządzenia. Urządzenia, które zostały wyprodukowane przez producenta określonego w tym polu, zostaną uwzględnione w wyborze.

  Nazwę producenta można wprowadzić w oknie właściwości urządzenia.

- **Numer seryjny**

  Cały sprzęt o numerze seryjnym określonym w tym polu zostanie uwzględniony w wyborze.

- **Numer ewidencyjny**

  Sprzęt o numerze inwentarzowym podanym w tym polu zostanie uwzględniony w wyborze.

- **Użytkownik**

  Cały sprzęt użytkownika określonego w tym polu zostanie uwzględniony w wyborze.

- **Lokalizacja**

  Lokalizacja urządzenia lub sprzętu (na przykład: w kwaterze głównej lub w oddziale firmy). Komputery lub inne urządzenia zainstalowane w lokalizacji określonej w tym polu zostaną uwzględnione w wyborze.

  Możesz opisać lokalizację urządzenia w dowolnym formacie w oknie właściwości tego urządzenia.

- **Częstotliwość procesora, w MHz**

  Zakres częstotliwości procesora. Urządzenia z procesorami odpowiadającymi zakresowi częstotliwości określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- **Wirtualne rdzenie procesora**

  Zakres liczby wirtualnych rdzeni w procesorze. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach (wszystkich) zostaną uwzględnione w wyborze.

- **Pojemność dysku twardego, w GB**

Zakres wartości rozmiaru dysku twardego urządzenia. Urządzenia z dyskami twardymi odpowiadającymi zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

- Rozmiar pamięci RAM, w MB

  Zakres wartości rozmiaru pamięci RAM urządzenia. Urządzenia z pamięcią RAM odpowiadającą zakresowi określonemu w tych polach wejściowych (wszystkich) zostaną uwzględnione w wyborze.

Maszyny wirtualne

W sekcji **Maszyny wirtualne** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w zależności od tego, czy są to maszyny wirtualne lub czy są one częścią infrastruktury pulpitu wirtualnego (VDI):

- Jest maszyną wirtualną

  Z listy rozwijalnej możesz wybrać następujące opcje:
  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są maszynami wirtualnymi.
  - **Tak**. Wyszukuje urządzenia, które są maszynami wirtualnymi.

- Typ maszyny wirtualnej

  Z listy rozwijalnej możesz wybrać producenta maszyny wirtualnej.

  Ta lista rozwijalna jest dostępna, jeśli wartość **Tak** lub **Nieważne** została wybrana na liście rozwijalnej **Jest maszyną wirtualną**.

- Część Virtual Desktop Infrastructure

  Z listy rozwijalnej możesz wybrać następujące opcje:
  - **Nieważne**.
  - **Nie**. Wyszukuje urządzenia, które nie są częścią Virtual Desktop Infrastructure.
  - **Tak**. Wyszukuje urządzenia, które są częścią Virtual Desktop Infrastructure (VDI).

Luki oraz aktualizacje

W sekcji **Luki oraz aktualizacje** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich źródłem Windows Update:

WUA został przełączony na Serwer administracyjny

Z listy rozwijalnej można wybrać jedną z następujących opcji wyszukiwania:

- **Tak**. Jeśli wybrano tę opcję, wyniki wyszukiwania będą uwzględniać urządzenia, które uzyskały aktualizacje poprzez Windows Update z Serwera administracyjnego.
- **Nie**. Jeśli wybrano tę opcję, wyniki będą uwzględniać urządzenia, które uzyskały aktualizacje za pośrednictwem Windows Update z innych źródeł.

Użytkownicy

W sekcji **Użytkownicy** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze według kont użytkowników, którzy logowali się do systemu operacyjnego.

- Ostatni użytkownik zalogowany do systemu

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik ostatnio logował się do systemu.

- Użytkownik zalogowany do systemu co najmniej raz

  Jeśli ta opcja jest włączona, kliknij przycisk **Przeglądaj**, aby określić konto użytkownika. Wyniki wyszukiwania zawierają urządzenia, na których określony użytkownik przynajmniej raz logował się do systemu.

Problemy mające wpływ na stan zarządzanych aplikacji

W sekcji **Problemy mające wpływ na stan zarządzanych aplikacji** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze według listy możliwych problemów wykrytych przez zarządzaną aplikację. Jeśli przynajmniej jeden problem, który wybrałeś, istnieje na urządzeniu, urządzenie zostanie uwzględnione w wyborze. Jeśli wybierzesz problem wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego problemu na wszystkich listach.

Opis stanu urządzenia

Możesz zaznaczyć opcje dla opisów stanów z zarządzanej aplikacji. Po odebraniu tych stanów, urządzenia zostaną uwzględnione w wyborze. Jeśli wybierzesz stan wymieniony dla kilku aplikacji, masz opcję automatycznego wyboru tego stanu na wszystkich listach.

Stan komponentów w zarządzanych aplikacjach

W sekcji **Stan komponentów w zarządzanych aplikacjach** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o stany komponentów w zarządzanych aplikacjach:

- Stan ochrony przed wyciekiem danych

  Wyszukiwanie urządzeń według stanu Ochrona przed wyciekaniem danych (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymano, Uruchomione, Niepowodzenie*).

- Stan ochrony serwerów współpracy

Wyszukiwanie urządzeń według stanu ochrony serwerów współpracy (*Brak danych z urządzenia*, *Zatrzymana*, *Uruchamianie, Wstrzymano*, *Uruchomione*, *Niepowodzenie*).

- **Stan ochrony antywirusowej serwerów pocztowych**

  Wyszukiwanie urządzeń według stanu ochrony dla serwerów pocztowych (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymano, Uruchomione, Niepowodzenie*).

- **Stan czujnika Endpoint Sensor**

  Wyszukiwanie urządzeń według stanu komponentu Endpoint Sensor (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymano, Uruchomione, Niepowodzenie*).

Szyfrowanie

Algorytm szyfrowania

Algorytm blokowego szyfru symetrycznego AES (Advanced Encryption Standard). Z listy rozwijalnej możesz wybrać długość klucza szyfrowania (56-bitowy, 128-bitowy, 192-bitowy lub 256-bitowy).

Dostępne wartości: *AES56*, *AES128*, *AES192* i *AES256*.

Segmenty chmury

W sekcji **Segmenty chmury** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o ich odpowiednie segmenty chmury:

- **Urządzenie znajduje się w segmencie chmury**

  Jeśli ta opcja jest włączona, możesz kliknąć przycisk **Przeglądaj**, aby określić przeszukiwany segment.

  Jeśli włączono także opcję **Włączając obiekty potomne**, wyszukiwanie jest uruchamiane na wszystkich obiektach potomnych określonego segmentu.

  Wyniki wyszukiwania zawierają tylko urządzenia z wybranego segmentu.

- **Urządzenie wykryte przy pomocy API**

Z listy rozwijalnej możesz wybrać, czy urządzenie jest wykrywane przez narzędzia API:

- **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.
- **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.
- **Google Cloud.** Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku Google Cloud.
- **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale nie może zostać wykryte przy użyciu API.
- **Brak wartości**. Warunek nie ma zastosowania.

Składniki aplikacji

Ta sekcja zawiera listę komponentów tych aplikacji, które posiadają odpowiednie wtyczki administracyjne, zainstalowane w Konsoli administracyjnej.

W sekcji **Składniki aplikacji** możesz określić kryteria uwzględniania urządzeń w wyborze zgodnie ze stanami i numerami wersji komponentów, które odpowiadają wybranej aplikacji:

- **Stan**

  Wyszukiwanie urządzeń zgodnie ze stanem komponentu wysłanym przez aplikację do Serwera administracyjnego. Możesz wybrać jeden z następujących stanów: *Brak danych z urządzenia*, *Zatrzymane*, *Uruchamianie*, *Wstrzymane*, *Uruchomione*, *Błąd* lub *Nie zainstalowano*. Jeśli wybrany komponent aplikacji zainstalowanej na zarządzanym urządzeniu posiada określony stan, urządzenie jest uwzględniane w wyborze urządzeń.

  Stany wysłane przez aplikacje:

  - *Uruchamianie*—komponent jest właśnie w procesie inicjalizacji.
  - *Uruchomione*—komponent jest włączony i działa poprawnie.
  - *Wstrzymane*—komponent został zawieszony, na przykład, po wstrzymaniu przez użytkownika ochrony w zarządzanej aplikacji.
  - *Błąd*—podczas działania komponentu wystąpił błąd.
  - *Zatrzymane*—komponent jest wyłączony i nie działa w tym momencie.
  - *Nie zainstalowano*—użytkownik nie wybrał komponentu do zainstalowania podczas konfigurowania niestandardowej instalacji aplikacji.

  W przeciwieństwie do pozostałych stanów, stan *Brak danych z urządzenia* nie jest wysyłany przez aplikacje. Ta opcja pokazuje, że aplikacje nie posiadają informacji o wybranym stanie komponentu. Na przykład, to może mieć miejsce, gdy wybrany komponent nie należy do żadnej z aplikacji zainstalowanych na urządzeniu lub gdy urządzenie jest wyłączone.

- **Wersja**

  Wyszukiwanie urządzeń zgodnie z numerem wersji komponentu, który wybierasz na liście. Możesz wpisać numer wersji, na przykład `3.4.1.0`, a następnie określić, czy wybrany komponent musi posiadać równą, wcześniejszą lub nowszą wersję. Możesz także skonfigurować wyszukiwanie wszystkich wersji, za wyjątkiem określonej.

Znaczniki urządzeń

Ta sekcja opisuje znaczniki urządzeń oraz zawiera instrukcje ich tworzenia i modyfikowania oraz ręcznego i automatycznego znakowania urządzeń.

Informacje o znacznikach urządzeń

Kaspersky Security Center umożliwia *znakowanie* urządzeń. Znacznik to etykieta urządzenia i może zostać użyty do grupowania, opisywania lub wyszukiwania urządzeń. Znaczniki przydzielone do urządzeń mogą być użyte do tworzenia wyborów, wyszukiwania urządzeń i rozdzielania urządzeń pomiędzy grupami administracyjnymi.

Urządzenia można znakować ręcznie lub automatycznie. Możesz użyć ręcznego znakowania, gdy chcesz oznakować pojedyncze urządzenie. Automatyczne znakowanie jest wykonywane przez Kaspersky Security Center zgodnie z określonymi regułami znakowania.

Urządzenia są znakowane automatycznie, gdy spełnione są określone reguły. Każdemu znacznikowi odpowiada pojedyncza reguła. Reguły są stosowane do właściwości sieciowych urządzenia, systemu operacyjnego, aplikacji zainstalowanych na urządzeniu i innych właściwości urządzenia. Na przykład, jeśli posiadasz infrastrukturę hybrydową maszyn fizycznych, instancji Amazon EC2 oraz maszyn wirtualnych Microsoft Azure, możesz skonfigurować regułę, która przypisze znacznik `[Azure]` do wszystkich maszyn wirtualnych Microsoft Azure. Następnie możesz użyć tego znacznika podczas tworzenia wyboru urządzeń; pomoże to w sortowaniu wszystkich maszyn wirtualnych Microsoft Azure i przypisaniu do nich zadania.

Znacznik jest automatycznie usuwany z urządzenia w następujących przypadkach:

- Jeśli urządzenie przestanie spełniać warunki reguły, która przypisuje znacznik.
- Jeśli reguła, która przypisuje znacznik, jest wyłączona lub została usunięta.

Lista znaczników oraz lista reguł na każdym Serwerze administracyjnym są niezależne od wszystkich pozostałych Serwerów administracyjnych, w tym głównego Serwera administracyjnego lub podległych wirtualnych Serwerów administracyjnych. Reguła jest stosowana tylko do urządzeń z tego samego Serwera administracyjnego, na którym reguła jest tworzona.

Tworzenie znacznika urządzenia

W celu utworzenia znacznika urządzenia:

1. W menu głównym przejdź do **Urządzenia** → **Znaczniki** → **Znaczniki urządzenia**.
2. Kliknij **Dodaj**.

   Zostanie otwarte okno nowego znacznika.

3. W polu **Znacznik** wprowadź nazwę znacznika.
4. Kliknij **Zapisz**, aby zachować zmiany.

Nowy znacznik pojawi się na liście znaczników urządzenia.

Zmienianie nazwy znacznika urządzenia

W celu zmiany nazwy znacznika urządzenia:

1. W menu głównym przejdź do **Urządzenia** → **Znaczniki** → **Znaczniki urządzenia**.
2. Kliknij nazwę znacznika, którego nazwę chcesz zmienić.
   Zostanie otwarte okno właściwości znacznika.
3. W polu **Znacznik** zmień nazwę znacznika.
4. Kliknij **Zapisz**, aby zachować zmiany.

Zaktualizowany znacznik pojawi się na liście znaczników urządzenia.

Usuwanie znacznika urządzenia

W celu usunięcia znacznika urządzenia:

1. W menu głównym przejdź do **Urządzenia** → **Znaczniki** → **Znaczniki urządzenia**.
2. Z listy wybierz znacznik urządzenia, który chcesz usunąć.
3. Kliknij przycisk **Usuń**.
4. W otwartym oknie kliknij **Tak**.

Znacznik urządzenia zostanie usunięty. Usunięty znacznik jest automatycznie usuwany ze wszystkich urządzeń, do których został przypisany.

Znacznik, który usunąłeś, nie zostanie usunięty automatycznie z reguł automatycznego znakowania. Po usunięciu znacznika, zostanie on przypisany do nowego urządzenia tylko wtedy, gdy urządzenie będzie spełniało wymagania reguły przypisującej znacznik.

Usunięty tag nie jest automatycznie usuwany z urządzenia, jeśli ten tag jest przypisany do urządzenia przez aplikację lub Agenta sieciowego. Aby usunąć tag z urządzenia, użyj narzędzia klscflag.

Przeglądanie urządzeń, do których przypisano znacznik

W celu przejrzenia urządzeń, do których przypisywany jest znacznik:

1. W menu głównym przejdź do **Urządzenia** → **Znaczniki** → **Znaczniki urządzenia**.
2. Kliknij odnośnik **Wyświetl urządzenia** obok znacznika, dla którego chcesz wyświetlić przypisane urządzenia.

   Jeśli obok znacznika nie ma odnośnika **Wyświetl urządzenia**, znacznik nie zostanie przypisany do żadnego urządzenia.

Wyświetlona lista urządzeń będzie zawierała tylko te urządzenia, do których został przypisany znacznik.

Aby wrócić do listy znaczników urządzenia, kliknij przycisk **Wstecz** w swojej przeglądarce.

Przeglądanie znaczników przydzielonych do urządzenia

W celu przejrzenia znaczników przydzielonych do urządzenia:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.
2. Kliknij nazwę urządzenia, którego znaczniki chcesz przejrzeć.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Znaczniki**.

Zostanie wyświetlona lista znaczników przypisanych do wybranego urządzenia.

Możesz przypisać inny znacznik do urządzenia lub usunąć już przypisany znacznik. Możesz także sprawdzić wszystkie znaczniki urządzenia, które znajdują się na Serwerze administracyjnym.

Ręczne oznaczanie urządzenia

W celu ręcznego przypisania znacznika do urządzenia:

1. Przejrzyj znaczniki przypisane do urządzenia, do którego chcesz przypisać inny znacznik.
2. Kliknij **Dodaj**.
3. W otwartym oknie wykonaj jedną z następujących czynności:
   - Aby utworzyć i przypisać nowy znacznik, wybierz **Utwórz nowy znacznik**, a następnie określ nazwę nowego znacznika.
   - Aby wybrać istniejący znacznik, wybierz **Przypisz istniejący znacznik**, a następnie, z listy rozwijalnej wybierz potrzebny znacznik.
4. Kliknij **OK**, aby zastosować zmiany.
5. Kliknij **Zapisz**, aby zachować zmiany.

Wybrany znacznik zostanie przypisany do urządzenia.

Usuwanie przydzielonego znacznika z urządzenia

W celu usunięcia znacznika z urządzenia:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.
2. Kliknij nazwę urządzenia, którego znaczniki chcesz przejrzeć.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Znaczniki**.
4. Zaznacz pole obok znacznika, który chcesz usunąć.
5. U góry listy kliknij przycisk **Wycofaj przypisanie znacznika**.
6. W otwartym oknie kliknij **Tak**.

Znacznik zostanie usunięty z urządzenia.

Znacznik urządzenia nieprzypisanego został usunięty. Jeśli chcesz, możesz usunąć go ręcznie.

Nie możesz ręcznie usunąć znaczników przypisanych do urządzenia przez aplikacje lub Agenta sieciowego. Aby usunąć te znaczniki, użyj narzędzia klscflag.

Wyświetlanie reguł automatycznego oznaczania urządzeń

W celu wyświetlenia reguł automatycznego znakowania urządzeń:

Wykonaj jedną z poniższych czynności:

- W menu głównym przejdź do **Urządzenia** → **Znaczniki** → **Reguły automatycznego znakowania**.
- W menu głównym przejdź do **Urządzenia** → **Znaczniki** → **Znaczniki urządzenia**, and then click the **Ustaw reguły automatycznego znakowania**.
- Przejrzyj znaczniki przypisane do urządzenia, a następnie kliknij przycisk **Ustawienia**.

Zostanie wyświetlona lista reguł automatycznego znakowania urządzeń.

Edytowanie reguły automatycznego znakowania urządzeń

W celu edytowania reguły automatycznego znakowania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.

2. Kliknij nazwę reguły, którą chcesz edytować.

   Zostanie otwarte okno ustawień reguły.

3. Edytuj ogólne właściwości reguły:

   a. W polu **Nazwa reguły** zmień nazwę reguły.

      Długość nazwy nie może wynosić więcej niż 256 znaków.

   b. Wykonaj jedną z poniższych czynności:

      - Włącz regułę, ustawiając przełącznik w pozycji **Reguła włączona**.
      - Wyłącz regułę, ustawiając przełącznik w pozycji **Reguła wyłączona**.

4. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz dodać nowy warunek, kliknij przycisk **Dodaj** i w otwartym oknie określ ustawienia nowego warunku.
   - Jeśli chcesz edytować istniejący warunek, kliknij nazwę warunku, który chcesz edytować, a następnie edytuj ustawienia warunku.
   - Jeśli chcesz usunąć warunek, zaznacz pole obok nazwy warunku, który chcesz usunąć, a następnie kliknij **Usuń**.

5. Kliknij przycisk **OK** w oknie ustawień warunków.

6. Kliknij **Zapisz**, aby zachować zmiany.

Edytowana reguła zostanie wyświetlona na liście.

Tworzenie reguły automatycznego znakowania urządzeń

W celu utworzenia reguły automatycznego znakowania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.

2. Kliknij **Dodaj**.

   Zostanie otwarte okno ustawień nowej reguły.

3. Skonfiguruj ogólne właściwości reguły:

   a. W polu **Nazwa reguły** wprowadź nazwę reguły.

      Długość nazwy nie może wynosić więcej niż 256 znaków.

   b. Wykonaj jedną z poniższych czynności:

      - Włącz regułę, ustawiając przełącznik w pozycji **Reguła włączona**.
      - Wyłącz regułę, ustawiając przełącznik w pozycji **Reguła wyłączona**.

c. W polu **Znacznik** wprowadź nazwę nowego znacznika urządzenia lub wybierz istniejące znaczniki urządzeń z listy.

Długość nazwy nie może wynosić więcej niż 256 znaków.

4. W sekcji warunków kliknij przycisk **Dodaj**, aby dodać nowy warunek.

Zostanie otwarte okno ustawień nowego warunku.

5. Wprowadź nazwę warunku.

Długość nazwy nie może wynosić więcej niż 256 znaków. Nazwa musi być unikatowa w obrębie reguły.

6. Skonfiguruj wyzwalanie reguły zgodnie z następującymi warunkami. Możesz określić kilka warunków.

- **Sieć**—właściwości sieci urządzenia, takie jak nazwa urządzenia w sieci Windows lub uwzględnienie urządzenia w domenie lub podsieci IP.

> Jeśli dla bazy danych używanej z Kaspersky Security Center ustawione jest sortowanie z rozróżnianiem wielkości liter, zachowaj wielkość liter podczas określania nazwy DNS urządzenia. W przeciwnym razie reguła automatycznego tagowania nie będzie działać.

- **Aplikacje**—obecność Agenta sieciowego na urządzeniu oraz typ, wersja i architektura systemu operacyjnego.
- **Maszyny wirtualne**—urządzenie należy do określonego typu maszyny wirtualnej.
- **Active Directory**—obecność urządzenia w jednostce organizacyjnej Active Directory i członkostwo urządzenia w grupie Active Directory.
- **Rejestr aplikacji**—obecność aplikacji różnych producentów na urządzeniu.

7. Kliknij **OK**, aby zachować zmiany.

Jeśli to konieczne, dla jednej reguły możesz ustawić kilka warunków. W tej sytuacji znacznik zostanie przypisany do urządzenia, jeśli spełnia przynajmniej jeden warunek.

8. Kliknij **Zapisz**, aby zachować zmiany.

Nowo utworzona reguła jest wymuszona na urządzeniach zarządzanych przez wybrany Serwer administracyjny. Jeśli ustawienia urządzenia spełniają warunki reguły, do urządzenia zostanie przydzielony znacznik.

Później reguła będzie stosowana w następujących przypadkach:

- Automatycznie i okresowo, w zależności od obciążenia na serwerze
- Po edytowaniu reguły
- Jeśli ręcznie uruchamiasz regułę
- Po wykryciu przez Serwer administracyjny zmian w ustawieniach urządzenia, które spełnia warunki reguły lub w ustawieniach grupy, która zawiera to urządzenie

Możesz utworzyć kilka reguł znakowania. Do jednego urządzenia może zostać przypisanych kilka znaczników, jeśli utworzyłeś kilka reguł znakowania i jeśli odpowiednie warunki tych reguł są spełnione w tym samym czasie. Listę wszystkich przydzielonych znaczników można przejrzeć we właściwościach urządzenia.

Uruchamianie reguł automatycznego znakowania urządzeń

Jeśli reguła jest uruchomiona, znacznik określony we właściwościach tej reguły zostanie przypisany do urządzeń, które spełniają warunki określone we właściwościach tej samej reguły. Możesz uruchamiać tylko aktywne reguły.

W celu uruchomienia reguł automatycznego znakowania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.
2. Zaznacz pola obok aktywnych reguł, które chcesz uruchomić.
3. Kliknij przycisk **Uruchom regułę**.

Wybrane reguły zostały uruchomione.

Usuwanie reguły automatycznego oznaczania urządzeń

W celu usunięcia reguły automatycznego oznaczania urządzeń:

1. Wyświetl reguły automatycznego oznaczania urządzeń.
2. Zaznacz pole obok reguły, którą chcesz usunąć.
3. Kliknij **Usuń**.
4. W otwartym oknie ponownie kliknij **Usuń**.

Wybrana reguła została usunięta. Znacznik, który został określony we właściwościach tej reguły, został wypisany ze wszystkich urządzeń, do których został przypisany.

Znacznik urządzenia nieprzypisanego został usunięty. Jeśli chcesz, możesz usunąć go ręcznie.

Zarządzanie znacznikami urządzeń za pomocą narzędzia klscflag

Ta sekcja zawiera informacje na temat przypisywania lub usuwania znaczników urządzeń za pomocą narzędzia klscflag.

Przypisywanie znacznika urządzenia

Pamiętaj, że musisz uruchomić narzędzie klscflag na urządzeniu klienckim, do którego chcesz przypisać znacznik.

Aby przypisać tag do urządzenia za pomocą narzędzia klscflag:

1. Wpisz następujące polecenie, korzystając z uprawnień administratora:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv
"[\" NAZWA ZNACZNIKA \"]" -svt TABLICA_T -ss "|typ_ss = \"SS_PRODINFO\";"
```

gdzie `NAZWA ZNACZNIKA` to nazwa znacznika, który chcesz przypisać do swojego urządzenia, na przykład:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "
[\" ENTERPRISE \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

2. Uruchom ponownie usługę Agenta sieciowego.

Wybrany znacznik zostanie przypisany do Twojego urządzenia. Aby upewnić się, że znacznik został pomyślnie przypisany, wyświetl znaczniki przypisane do urządzenia.

Alternatywnie możesz ręcznie przypisać znaczniki urządzeń.

Usuwanie znacznika urządzenia

Jeśli znacznik został przypisany do Twojego urządzenia przez aplikację lub Agenta sieciowego, nie możesz usunąć tego znacznika ręcznie. W takim przypadku użyj narzędzia klscflag, aby usunąć przypisany znacznik z urządzenia.

Pamiętaj, że musisz uruchomić narzędzie klscflag na urządzeniu klienckim, z którego chcesz usunąć znacznik.

Aby usunąć znacznik z urządzenia za pomocą narzędzia klscflag:

1. Wpisz następujące polecenie, korzystając z uprawnień administratora:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "
[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

2. Uruchom ponownie usługę Agenta sieciowego.

Znacznik zostanie usunięty z urządzenia.

Profile i profile zasad

W Kaspersky Security Center Web Console możesz tworzyć zasady dla aplikacji Kaspersky. Ta sekcja opisuje profile i profile zasad, a także zawiera instrukcje dotyczące ich tworzenia i modyfikowania.

Informacje o zasadach i profilach zasad

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

Stan zasady

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

Zasady działają zgodnie z następującymi regułami:

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

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

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

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

Profile zasad działają zgodnie z następującymi regułami:

- Profil zasad zaczyna obowiązywać, gdy wystąpi określony warunek aktywacji.
- Profile zasad zawierają wartości ustawień, które różnią się od ustawień zasad.
- Aktywacja profilu zasad zmienia obowiązujące ustawienia zarządzanego urządzenia.
- Zasada może zawierać maksymalnie 100 profili zasad.

Informacje o blokadzie i zablokowanych ustawieniach

Każde ustawienie zasady ma ikonę przycisku blokady (🔒). Poniższa tabela przedstawia stany przycisków blokady:

Stany przycisków blokady

Stan	Opis
	Jeśli obok ustawienia jest wyświetlana otwarta kłódka, a przycisk przełącznika jest wyłączony, ustawienie nie jest określone w zasadzie. Użytkownik może zmienić te ustawienia w interfejsie zarządzanej aplikacji. Tego typu ustawienia nazywane są *odblokowanymi*.
	Jeśli obok ustawienia jest wyświetlana zamknięta kłódka, a przycisk przełącznika jest włączony, ustawienie jest stosowane do urządzeń, na których zasada jest wymuszana. Użytkownik nie może zmodyfikować wartości tych ustawień w interfejsie zarządzanej aplikacji. Tego typu ustawienia nazywane są *zablokowanymi*.

Zdecydowanie zalecamy zamknięcie blokad dla ustawień zasad, które chcesz zastosować na zarządzanych urządzeniach. Odblokowane ustawienia zasady można ponownie przypisać przez ustawienia aplikacji Kaspersky na zarządzanym urządzeniu.

Możesz użyć przycisku blokady, aby wykonać następujące czynności:

- Blokowanie ustawień dla zasady podgrupy administracyjnej

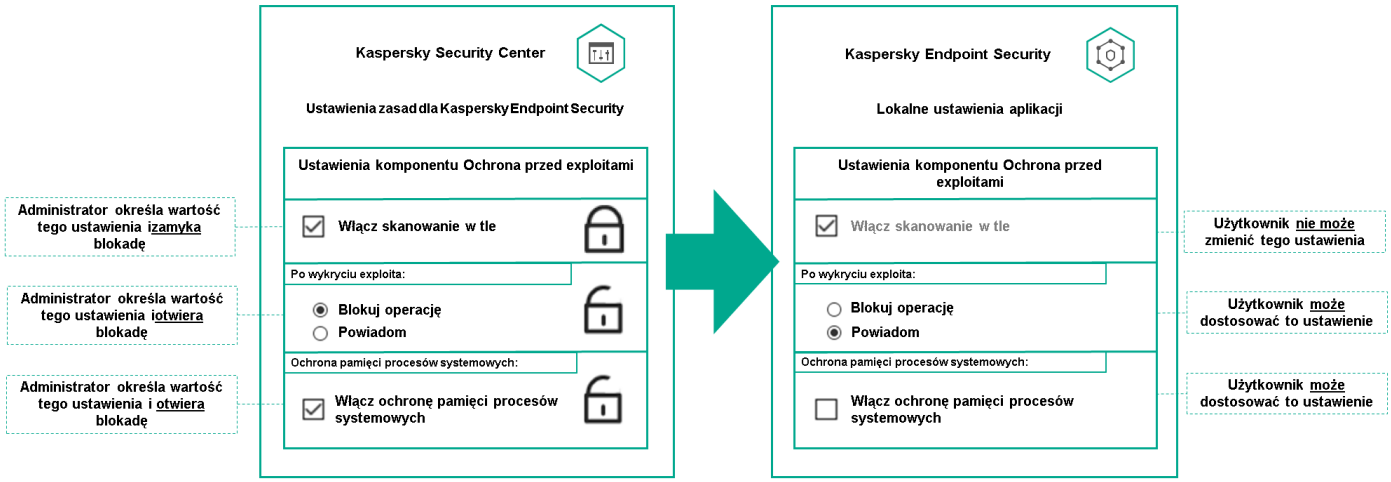
- Blokowanie ustawień aplikacji Kaspersky na zarządzanym urządzeniu

W ten sposób zablokowane ustawienie jest używane do implementacji obowiązujących ustawień na zarządzanym urządzeniu.

Proces skutecznego wdrażania ustawień obejmuje następujące działania:

- Zarządzane urządzenie stosuje wartości ustawień aplikacji Kaspersky.
- Zarządzane urządzenie stosuje zablokowane wartości ustawień zasady.

Zasada i zarządzana aplikacja Kaspersky zawierają ten sam zbiór ustawień. Po skonfigurowaniu ustawień zasady, wartości ustawień aplikacji Kaspersky ulegają zmianie na zarządzanym urządzeniu. Użytkownik nie może dostosować zablokowanych ustawień na zarządzanym urządzeniu (patrz rysunek poniżej):



Blokady i ustawienia aplikacji Kaspersky

Dziedziczenie zasad i profili zasad

Ta sekcja zawiera informacje o hierarchii i dziedziczeniu zasad oraz profilach zasad.

Hierarchia profili

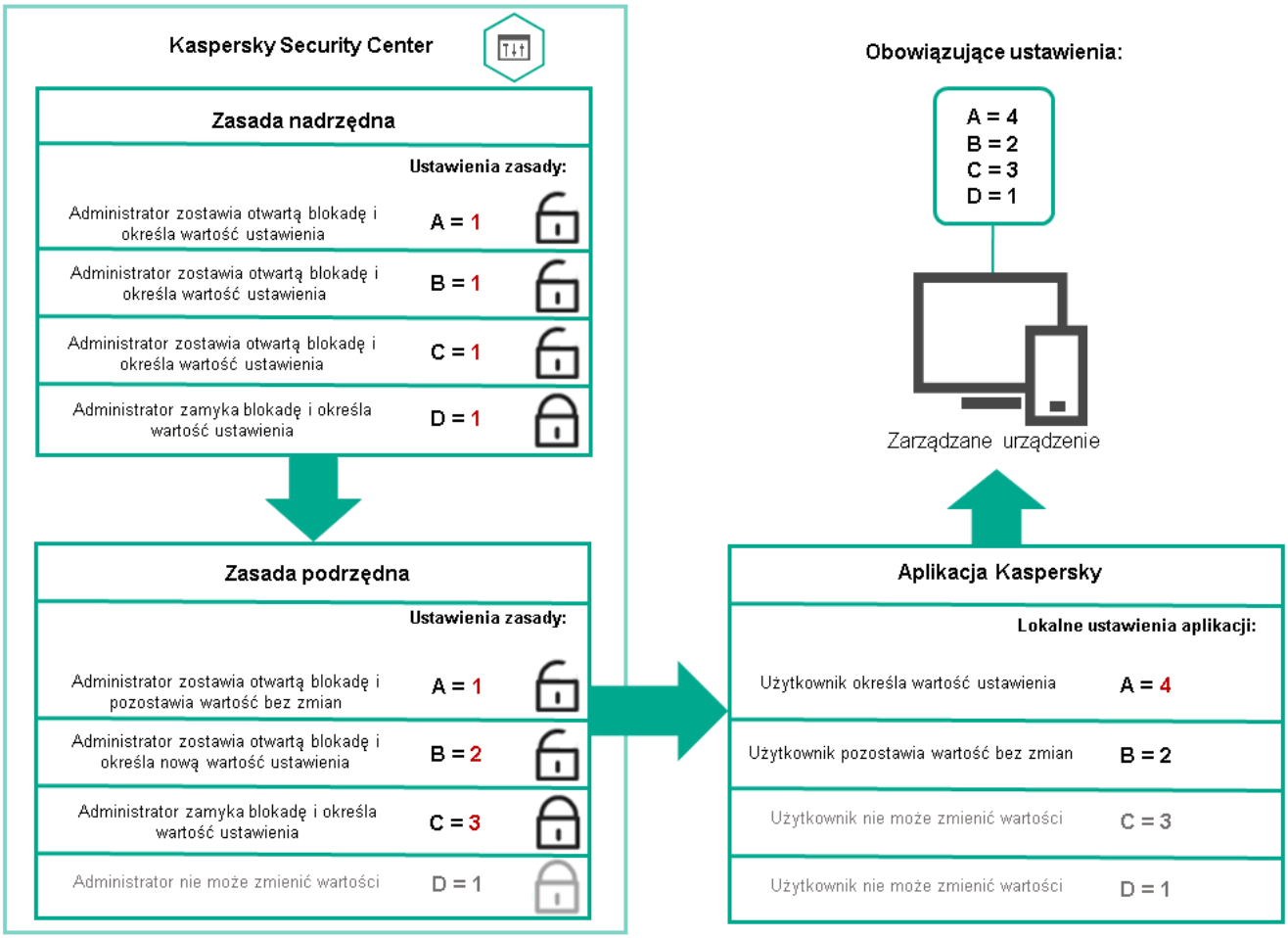
Jeśli różne urządzenia wymagają różnych ustawień, możesz zorganizować je w grupy administracyjne.

Możesz określić zasadę dla pojedynczej grupy administracyjnej. Ustawienia zasad mogą być *dziedziczone*. Dziedziczenie oznacza odbieranie wartości ustawień zasad w podgrupach (grupach podrzędnych) z zasady grupy administracyjnej wyższego poziomu (nadrzędnej).

Dalej profil dla grupy nadrzędnej jest też zwany *zasadą nadrzędną*. Dalej zasada dla podgrupy (grupy podrzędnej) jest też zwana *zasadą podrzędną*.

Domyślnie co najmniej jedna grupa zarządzane urządzenia istnieje na Serwerze administracyjnym. Jeśli chcesz utworzyć grupy niestandardowe, są one tworzone jako podgrupy (grupy podrzędne) w ramach grupy zarządzane urządzenia.

Zasady tej samej aplikacji oddziałują na siebie zgodnie z hierarchią grup administracyjnych. Zablokowane ustawienia z zasady grupy administracyjnej wyższego poziomu (nadrzędnej) spowodują ponowne przypisanie wartości ustawień zasad podgrupy (patrz rysunek poniżej).

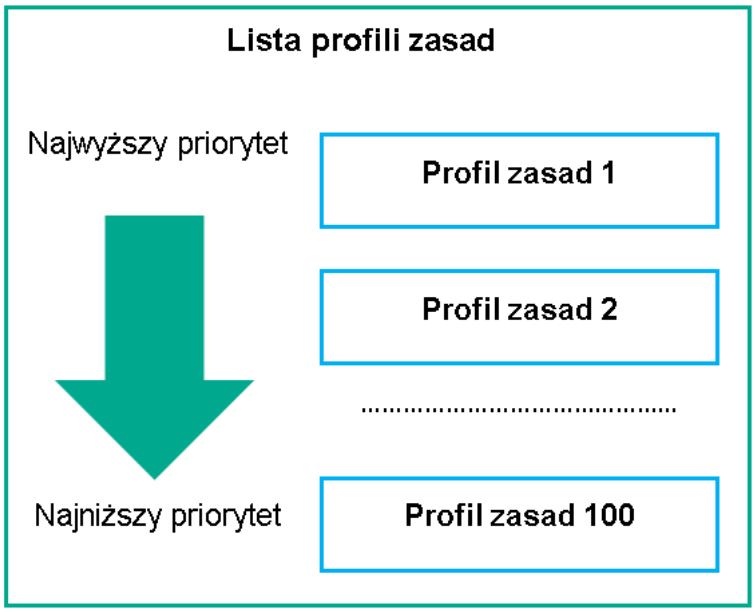


Hierarchia profili

Profile zasad w hierarchii zasad

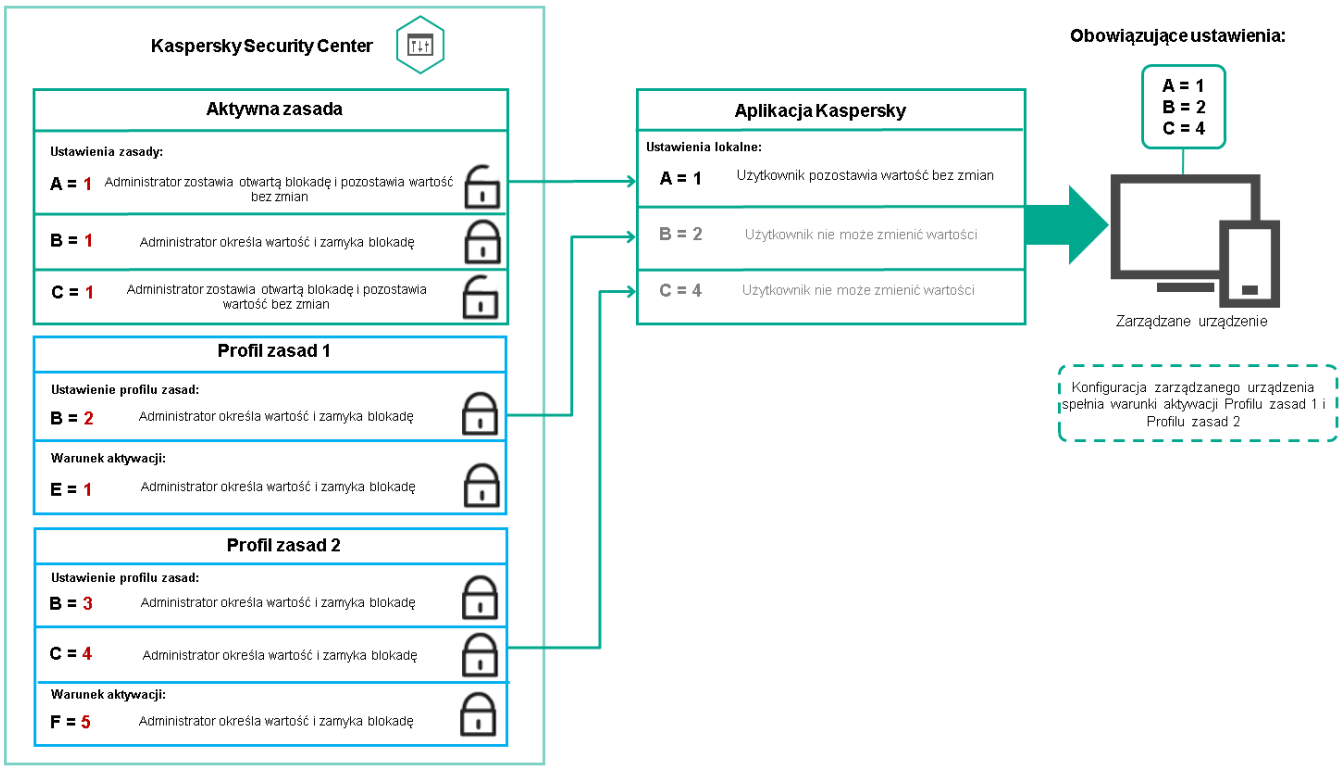
Profile zasad mają następujące warunki przypisywania priorytetów:

- Pozycja profilu na liście profili zasad wskazuje jego priorytet. Możesz zmienić priorytet profilu zasad. Najwyższa pozycja na liście oznacza najwyższy priorytet (patrz rysunek poniżej).



Definicja priorytetu profilu zasad

- Warunki aktywacji profili zasad nie są od siebie zależne. Jednocześnie można aktywować kilka profili zasad. Jeśli kilka profili zasad wpływa na to samo ustawienie, urządzenie przyjmuje wartość ustawienia z profilu zasad o najwyższym priorytecie (patrz rysunek poniżej).



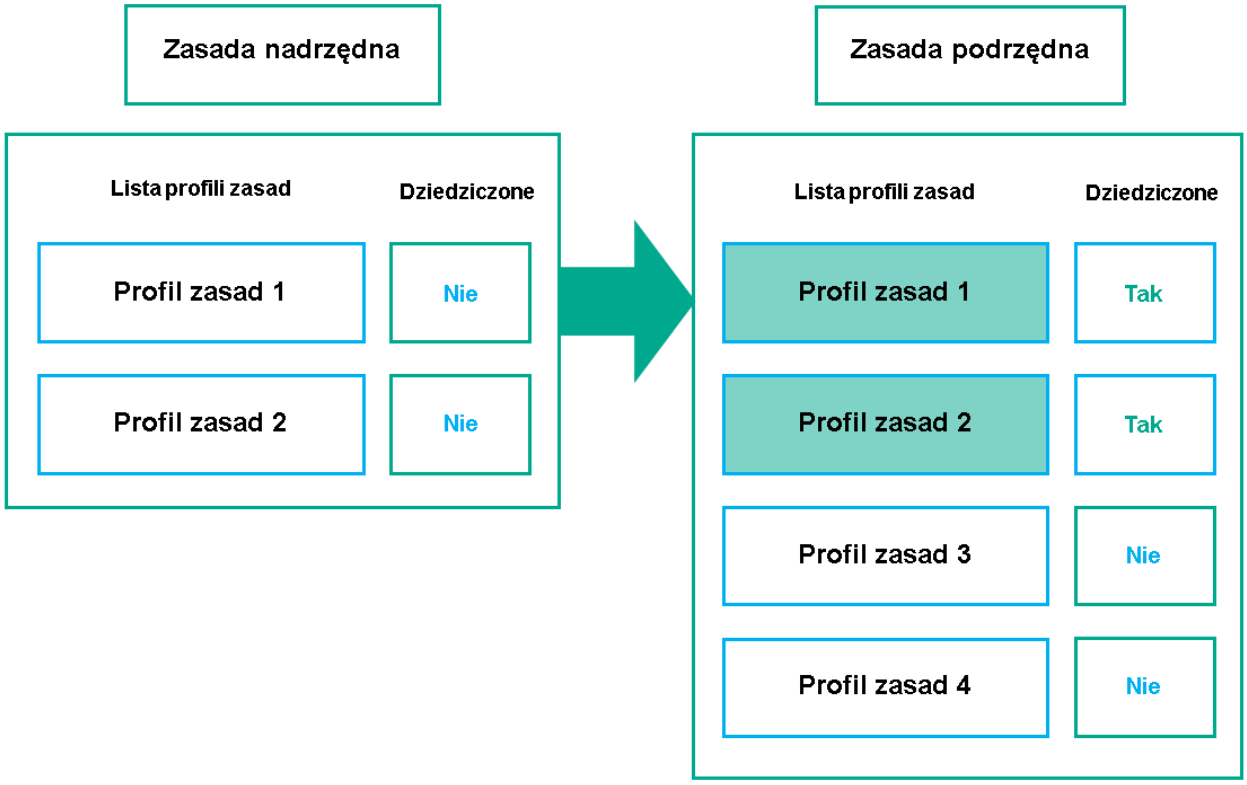
Konfiguracja zarządzanego urządzenia spełnia warunki aktywacji kilku profili zasad

Profile zasad w hierarchii dziedziczenia

Profile zasad z zasad różnych poziomów hierarchii spełniają następujące warunki:

- Zasada niższego poziomu dziedziczy profile zasad z zasady wyższego poziomu. Profil zasad odziedziczony z zasady wyższego poziomu uzyskuje wyższy priorytet niż poziom oryginalnego profilu zasad.

- Nie można zmienić priorytetu odziedziczonego profilu zasad (zobacz poniższy rysunek).

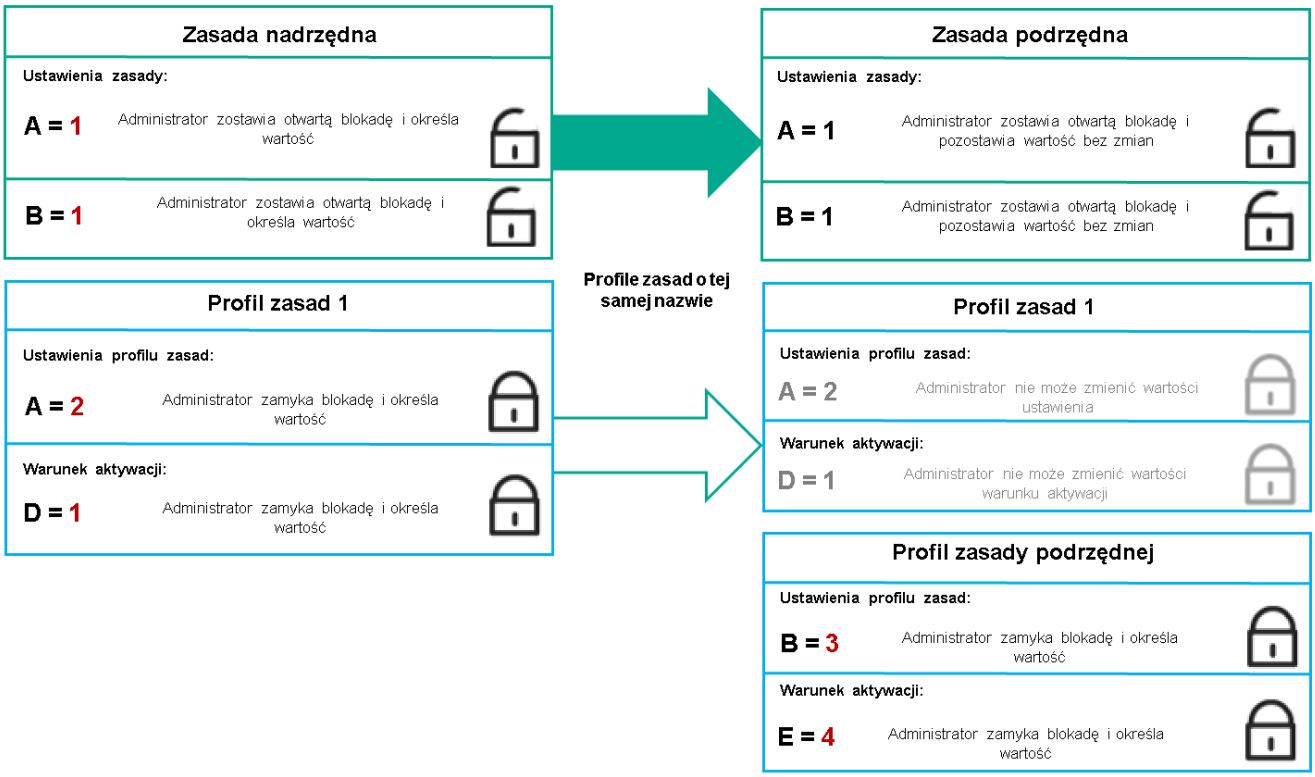


Dziedziczenie profili zasad

Profile zasad o tej samej nazwie

Jeśli istnieją dwie zasady o tych samych nazwach na różnych poziomach hierarchii, te zasady działają zgodnie z następującymi regułami:

- Ustawienia zablokowane i warunek aktywacji profilu zasad wyższego poziomu zmieniają ustawienia i warunek aktywacji profilu zasad niższego poziomu (patrz rysunek poniżej).



Profil podrzędny dziedziczy wartości ustawień z nadrzędnego profilu zasad

- Ustawienia odblokowane i warunek aktywacji profilu zasad wyższego poziomu nie zmieniają ustawień i warunku aktywacji profilu zasad niższego poziomu.

Implementacja ustawień na zarządzanym urządzeniu

Implementację obowiązujących ustawień na zarządzanym urządzeniu można opisać w następujący sposób:

- Wartości wszystkich ustawień, które nie zostały zablokowane, są pobierane z zasady.
- Następnie są nadpisywane wartościami ustawień zarządzanej aplikacji.
- Następnie stosowane są zablokowane wartości ustawień z obowiązującej zasady. Zablokowane wartości ustawień zmieniają wartości odblokowanych obowiązujących ustawień.

Zarządzanie profilami

Ta sekcja opisuje zarządzanie zasadami i zawiera informacje o przeglądaniu listy zasad, tworzeniu zasady, modyfikowaniu zasady, kopiowaniu zasady, przenoszeniu zasady, wymuszonej synchronizacji, przeglądaniu wykresu stanu dystrybucji zasad i usuwaniu zasady.

Przeglądanie listy zasad

Możesz przejrzeć listy zasad utworzonych dla Serwera administracyjnego lub dla dowolnej grupy administracyjnej.

W celu wyświetlenia listy zasad:

1. W menu głównym przejdź do **Urządzenia** → **Hierarchia grup**.
2. W strukturze grupy administracyjnej należy wybrać grupę administracyjną, dla której chcesz przejrzeć listę zasad.

Lista zasad zostanie wyświetlona w postaci tabeli. Jeśli nie ma zasad, tabela jest pusta. Możesz wyświetlać lub ukrywać kolumny tabeli, zmieniać ich kolejność, przeglądać tylko wiersze, które zawierają określoną przez Ciebie wartość, lub korzystać z wyszukiwania.

Tworzenie zasady

Możesz tworzyć zasady, a także modyfikować i usuwać istniejące zasady.

W celu utworzenia zasady:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij **Dodaj**.

   Zostanie otwarte okno **Wybierz aplikację**.
3. Wybierz aplikację, dla której chcesz utworzyć zasadę.
4. Kliknij **Dalej**.

   Zostanie otwarte okno ustawień nowej zasady na zakładce **Ogólne**.
5. Jeśli chcesz, zmień domyślną nazwę, domyślny stan oraz domyślne ustawienia dziedziczenia zasady.
6. Wybierz zakładkę **Ustawienia aplikacji**.

   Lub kliknij **Zapisz** i zakończ działanie. Zasada pojawi się na liście zasad i będziesz mógł w późniejszym czasie edytować jego ustawienia.
7. Na zakładce **Ustawienia aplikacji**, w lewej części okna wybierz żądaną kategorię, a w prawej części okna zmień ustawienia zasady. Możesz edytować ustawienia zasady w każdej kategorii (sekcja).

   Zestaw ustawień zależy od aplikacji, dla której tworzysz zasadę. Więcej informacji można znaleźć w:

   - Konfiguracja Serwera administracyjnego
   - Ustawienia zasady Agenta sieciowego
   - Dokumentacja do Kaspersky Endpoint Security for Windows

   Szczegółowe informacje dotyczące ustawień innych aplikacji zabezpieczających można znaleźć w dokumentacji dla odpowiedniej aplikacji.

   Podczas edytowania ustawień możesz kliknąć **Anuluj**, aby anulować ostatnie działanie.
8. Kliknij **Zapisz**, aby zapisać zasadę.

Zasada zostanie wyświetlona na liście zasad.

Modyfikowanie zasady

W celu zmodyfikowania zasady:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij zasadę, którą chcesz zmodyfikować.

   Zostanie otwarte okno ustawień zasady.
3. Określ ustawienia główne oraz ustawienia aplikacji, dla której tworzysz zasadę. Więcej informacji można znaleźć w:

   - Konfiguracja Serwera administracyjnego
   - Ustawienia zasady Agenta sieciowego
   - Dokumentacja do Kaspersky Endpoint Security for Windows

   Szczegółowe informacje dotyczące ustawień innych aplikacji zabezpieczających można znaleźć w dokumentacji dla tej aplikacji.
4. Kliknij **Zapisz**.

Zmiany wprowadzone w zasadzie zostaną zapisane we właściwościach zasady i pojawią się w sekcji **Historia rewizji**.

Ogólne ustawienia zasady

Ogólne

Na zakładce **Ogólne** możesz zmodyfikować stan profilu oraz określić dziedziczenie ustawień profilu:

- W sekcji **Stan zasady** możesz wybrać jeden z trybów zasady:
  - **Aktywny**

    Jeśli wybrano tę opcję, zasada jest aktywna.

    Domyślnie opcja ta jest zaznaczona.
  - **Użytkownik mobilny**

    Jeżeli ta opcja jest zaznaczona, zasada stanie się aktywna, gdy urządzenie znajdzie się poza siecią korporacyjną.
  - **Nieaktywny**

Jeśli ta opcja jest zaznaczona, zasada stanie się nieaktywna, ale wciąż będzie przechowywana w folderze **Zasady**. Jeśli jest to wymagane, zasadę można aktywować.

- W grupie ustawień **Dziedziczenie ustawień** możesz skonfigurować dziedziczenie zasady:
  - Dziedzicz ustawienia z zasady nadrzędnej

    Jeśli ta opcja jest włączona, wartości ustawień zasady są dziedziczone z zasady grupy najwyższego poziomu, są więc zablokowane.

    Domyślnie opcja ta jest włączona.

  - Wymuś dziedziczenie ustawień w zasadach podrzędnych

    Jeśli ta opcja jest włączona, po zastosowaniu zmian w zasadzie zostaną wykonane następujące czynności:
    - Wartości ustawień zasady zostaną rozesłane do zasad podgrup administracyjnych, czyli do zasad podrzędnych.
    - Opcja **Dziedzicz ustawienia z zasady nadrzędnej** będzie automatycznie włączona w podsekcji **Dziedziczenie ustawień** sekcji **Ogólne** okna właściwości każdej zasady podrzędnej.

    Jeśli ta opcja jest włączona, ustawienia zasad podrzędnych są zablokowane.

    Domyślnie opcja ta jest wyłączona.

Konfiguracja zdarzenia

Zakładka **Konfiguracja zdarzenia** umożliwia skonfigurowanie zapisywania zdarzeń oraz powiadamiania o zdarzeniach. Zdarzenia są grupowane według istotności na następujących zakładkach:

- **Krytyczny**

  Sekcja **Krytyczny** nie jest wyświetlana we właściwościach profilu Agenta sieciowego.
- **Błąd funkcjonalny**
- **Ostrzeżenie**
- **Informacja**

W każdej sekcji, lista wyświetla typy zdarzeń oraz domyślny czas przechowywania zdarzeń na Serwerze administracyjnym (w dniach). Kliknięcie typu zdarzenia umożliwia określenie następujących ustawień:

- **Rejestracja zdarzenia**

  Możesz określić ilość dni przechowywania zdarzenia oraz wybrać miejsce przechowywania zdarzenia:
  - **Eksportuj do systemu SIEM przez Dziennik systemu**
  - **Przechowuj w systemowym dzienniku zdarzeń urządzenia**
  - **Przechowuj w systemowym dzienniku zdarzeń Serwera administracyjnego**
- **Powiadomienia o zdarzeniu**

Możesz wybrać, jeśli chcesz być powiadamiany o zdarzeniu w jeden z następujących sposobów:

- **Powiadom przez e-mail**
- **Powiadom przez SMS**
- **Powiadom, uruchamiając plik wykonywalny lub skrypt**
- **Powiadom przez SNMP**

Domyślnie, używane są ustawienia powiadamiania, określone na zakładce Właściwości Serwera administracyjnego (takie, jak adres odbiorcy). Jeśli chcesz, możesz zmienić te ustawienia na zakładkach: **E-mail**, **SMS** i **Plik wykonywalny do uruchomienia**.

Historia rewizji

Zakładka **Historia rewizji** umożliwia przeglądanie listy rewizji profilu i wycofanie zmian wprowadzonych do profilu (jeśli to konieczne).

Włączanie i wyłączanie opcji dziedziczenia zasady

Aby włączyć lub wyłączyć opcję dziedziczenia w zasadzie:

1. Otwórz wymaganą zasadę.
2. Otwórz zakładkę **Ogólne**.
3. Włącz lub wyłącz dziedziczenie zasad:
   - Jeśli włączysz opcję **Dziedzicz ustawienia z zasady nadrzędnej** w zasadzie podrzędnej i administrator zablokuje niektóre ustawienia w zasadzie nadrzędnej, wówczas nie będzie można zmienić tych ustawień w zasadzie podrzędnej.
   - Jeśli wyłączysz opcję **Dziedzicz ustawienia z zasady nadrzędnej** w zasadzie podrzędnej, wówczas możesz zmienić wszystkie ustawienia w zasadzie podrzędnej nawet wtedy, gdy niektóre ustawienia są zablokowane w zasadzie nadrzędnej.
   - Jeśli włączysz opcję **Wymuś dziedziczenie ustawień w zasadach podrzędnych** w grupie nadrzędnej, spowoduje to włączenie opcji **Dziedzicz ustawienia z zasady nadrzędnej** dla każdej zasady podrzędnej. W tym przypadku nie możesz wyłączyć tej opcji dla żadnego profilu potomnego. Wszystkie ustawienia, które są zablokowane w zasadzie nadrzędnej, są dziedziczone w grupach podrzędnych w sposób wymuszony i nie możesz zmienić tych ustawień w grupach podrzędnych.
4. Kliknij przycisk **Zapisz**, aby zapisać zmiany, lub kliknij przycisk **Anuluj**, aby odrzucić zmiany.

Domyślnie, opcja **Dziedzicz ustawienia z zasady nadrzędnej** jest włączona dla nowego profilu.

Jeśli zasada zawiera profile, wszystkie zasady podrzędne dziedziczą te profile.

Kopiowanie zasady

Możesz skopiować profile z jednej grupy administracyjnej do innej.

W celu skopiowania profilu do innej grupy administracyjnej:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Zaznacz pole obok profilu (profili), który (które) chcesz skopiować.
3. Kliknij przycisk **Kopiuj**.

   W prawej części okna pojawi się drzewo grup administracyjnych.
4. Z drzewa wybierz grupę docelową, czyli grupę, do której chcesz skopiować profil (profile).
5. W dolnej części okna kliknij przycisk **Kopiuj**.
6. Kliknij **OK**, aby potwierdzić działanie.

Profil (profile) zostanie skopiowany do grupy docelowej ze wszystkimi swoimi zasadami. Stan każdego skopiowanego profilu w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

Jeżeli profil z nazwą podobną do nazwy nowo przeniesionego profilu znajduje się już w grupie docelowej, do nazwy nowo przeniesionego profilu zostanie dodany przyrostek (<kolejny numer>), na przykład: (1).

Przenoszenie zasady

Możesz przenieść profile z jednej grupy administracyjnej do innej. Na przykład, chcesz usunąć grupę, ale chcesz używać jej profili dla innej grupy. W tym przypadku można przenieść profil ze starszej grupy do nowej zanim usuniesz starszą grupę.

W celu przeniesienia profilu do innej grupy administracyjnej:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Zaznacz pole obok profilu (profili), który (które) chcesz przenieść.
3. Kliknij przycisk **Przenieś**.

   W prawej części okna pojawi się drzewo grup administracyjnych.
4. Z drzewa wybierz grupę docelową, czyli grupę, do której chcesz przenieść profil (profile).
5. W dolnej części okna kliknij przycisk **Przenieś**.
6. Kliknij **OK**, aby potwierdzić działanie.

Jeśli zasada nie jest dziedziczona z grupy źródłowej, zostaje przeniesiona do grupy docelowej ze wszystkimi swoimi profilami. Stan profilu w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

Jeśli profil jest dziedziczony z grupy źródłowej, pozostanie w grupie źródłowej. Zostanie skopiowany do grupy docelowej ze wszystkimi swoimi zasadami. Stan profilu w grupie docelowej będzie **Nieaktywny**. W dowolnym momencie możesz zmienić stan na **Aktywny**.

Jeżeli profil z nazwą podobną do nazwy nowo przeniesionego profilu znajduje się już w grupie docelowej, do nazwy nowo przeniesionego profilu zostanie dodany przyrostek (<kolejny numer>), na przykład: (1).

Eksportowanie profilu

Kaspersky Security Center umożliwia zapisanie profilu, jego ustawień i profili zasad w pliku KLP. Możesz użyć tego pliku KLP do zaimportowania zapisanej zasady zarówno do Kaspersky Security Center Windows, jak i Kaspersky Security Center Linux.

W celu wyeksportowania profilu:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Zaznacz pole obok zasady, którą chcesz wyeliminować.

   Nie można jednocześnie eksportować wielu zasad. Jeśli wybierzesz więcej niż jedną zasadę, przycisk **Eksportuj** będzie nieaktywny.
3. Kliknij przycisk **Eksportuj**.
4. W otwartym oknie **Zapisz jako** określ nazwę i ścieżkę dostępu pliku profilu. Kliknij przycisk **Zapisz**.

   Okno **Zapisz jako** jest wyświetlane tylko wtedy, gdy korzystasz z przeglądarki Google Chrome, Microsoft Edge lub Opera. Jeśli używasz innej przeglądarki, plik zasady jest automatycznie zapisywany w folderze **Pobrane**.

Importowanie profilu

Kaspersky Security Center umożliwia importowanie profilu z pliku KLP. Plik KLP zawiera wyeksportowaną zasadę, jej ustawienia oraz profile zasad.

W celu zaimportowania profilu:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij przycisk **Importuj**.
3. Kliknij przycisk **Przeglądaj**, aby wybrać plik zasad, który chcesz zaimportować.
4. W otwartym oknie określ ścieżkę do pliku zasady KLP, a następnie kliknij przycisk **Otwórz**. Pamiętaj, że możesz wybrać tylko jeden plik zasady.

   Rozpoczyna się przetwarzanie zasady.
5. Po pomyślnym przetworzeniu zasady wybierz Grupa administracyjna, do których chcesz przypisać zasadę.
6. Kliknij przycisk **Zakończone**, aby zakończyć import zasad.

Pojawi się powiadomienie z wynikami importu. Jeśli zasada została pomyślnie zaimportowana, możesz kliknąć łącze **Szczegóły**, aby wyświetlić właściwości zasady.

Po pomyślnym imporcie zasada zostanie wyświetlona na liście zasad. Importowane są również ustawienia i profile zasad. Niezależnie od statusu zasady, który został wybrany podczas eksportu, importowana zasada jest nieaktywna. Możesz zmienić stan zasady we właściwościach zasady.

Jeżeli nowo importowana zasada ma nazwę identyczną z nazwą istniejącej zasady, nazwa importowanej zasady jest rozszerzana o indeks **(<następny numer kolejny>)**, na przykład: **(1)**, **(2)**.

Przeglądanie wykresu stanu dystrybucji zasad

W Kaspersky Security Center możesz przejrzeć stan zastosowania zasady na każdym urządzeniu w wykresie stanu dystrybucji zasady.

W celu wyświetlenia stanu dystrybucji zasady na każdym urządzeniu:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Zaznacz pole obok nazwy zasady, dla której chcesz przejrzeć stan dystrybucji na urządzeniach.
3. W wyświetlonym menu wybierz odnośnik **Dystrybucja**.

   Zostanie otwarte okno **Wyniki dystrybucji <nazwa zasady>**.
4. W otwartym oknie **Wyniki dystrybucji <nazwa zasady>** zostanie wyświetlony **Opis stanu** zasady.

Możesz zmienić liczbę wyników wyświetlanych na liście z dystrybucją zasady. Maksymalna liczba urządzeń to 100 000.

W celu zmiany liczby urządzeń wyświetlanych na liście z wynikami dystrybucji zasady:

1. W menu głównym przejdź do ustawień konta i wybierz **Opcje interfejsu**.
2. W sekcji **Ogranicz urządzenia wyświetlane w wynikach dystrybucji zasady** wprowadź liczbę urządzeń (do 100 000).

   Domyślnie ustawiona jest liczba 5000.
3. Kliknij **Zapisz**.

   Ustawienia zostaną zapisane i zastosowane.

Aktywowanie zasady automatycznie po wystąpieniu zdarzenia Epidemia wirusa

W celu skonfigurowania zasady tak, aby była aktywowana automatycznie po wystąpieniu Epidemii wirusa:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.
2. Wybierz sekcję **Epidemia wirusa**.
3. W prawej części okna kliknij odnośnik **Skonfiguruj zasady, które zostaną aktywowane po wystąpieniu epidemii wirusa**.

   Zostanie otwarte okno **Aktywacja zasady**.
4. W sekcji dotyczącej komponentu, który wykrywa epidemię wirusa—Ochrona antywirusowa stacji roboczych i serwerów plików, Ochrona antywirusowa dla serwerów pocztowych lub Ochrona antywirusowa bram internetowych—wybierz przycisk opcji obok żądanego wpisu, a następnie kliknij **Dodaj**.

Zostanie otwarte okno z grupą administracyjną **Zarządzane urządzenia**.

5. Kliknij ikonę strzałki (>) obok **Zarządzane urządzenia**.

   Zostanie wyświetlona hierarchia grup administracyjnych i ich zasad.

6. W hierarchii grup administracyjnych i ich zasad kliknij nazwę zasady lub zasad, które są aktywowane w przypadku wykrycia epidemii wirusa.

   Aby wybrać wszystkie zasady na liście lub w grupie, zaznacz pole obok żądanej nazwy.

7. Kliknij przycisk **Zapisz**.

   Okno z hierarchią grup administracyjnych i ich zasad zostało zamknięte.

Wybrane zasady są dodawane do listy zasad, które są aktywowane po wykryciu epidemii wirusa. Wybrane zasady są aktywowane w momencie wystąpienia epidemii wirusa, niezależnie od tego, czy są aktywne czy nie.

Jeśli profil został aktywowany po wystąpieniu zdarzenia Epidemia wirusa, możesz wrócić do poprzedniej zasady tylko przy użyciu trybu ręcznego.

Usuwanie zasady

Możesz usunąć profil, jeśli już go nie potrzebujesz. Możesz usunąć tylko ten profil, który nie jest dziedziczony w określonej grupie administracyjnej. Jeśli profil został odziedziczony, możesz go usunąć tylko w grupie wyższego poziomu, dla której został utworzony.

W celu usunięcia profilu:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.

2. Zaznacz pole obok profilu zasad, który chcesz usunąć, a następnie kliknij **Usuń**.

   Przycisk **Usuń** stanie się niedostępny (przyciemniony), jeśli wybierzesz profil dziedziczony.

3. Kliknij **OK**, aby potwierdzić działanie.

Profil jest usuwany ze wszystkimi swoimi zasadami.

Zarządzanie profilami zasad

Ta sekcja opisuje zarządzanie profilami zasad i zawiera informacje o wyświetlaniu profili zasad, zmienianiu priorytetu profili zasad, tworzeniu profili zasad, modyfikowaniu profili zasad, kopiowaniu profili zasad, tworzeniu reguł aktywacji profili zasad i usuwaniu profili zasad.

Przeglądanie profili zasad

W celu przejrzenia profili zasad:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.

2. Kliknij nazwę zasady, której profile chcesz przejrzeć.

   Okno właściwości zasady zostanie otwarte na wybranej zakładce **Ogólne**.

3. Otwórz zakładke **Profile zasad**.

Lista profili zasad zostanie wyświetlona w postaci tabeli. Jeśli zasada nie zawiera profili, pojawi się pusta tabela.

Zmiana priorytetu profilu zasad

W celu zmiany priorytetu profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** zaznacz pole obok profilu zasad, dla którego chcesz zmienić priorytet.

3. Ustaw nową pozycję profilu zasad na liście, klikając **Nadaj priorytet** lub **Usuń priorytet**.

   Im wyżej profil zasad znajduje się na liście, tym wyższy jego priorytet.

4. Kliknij przycisk **Zapisz**.

Priorytet wybranego profilu zasad zostanie zmieniony i zastosowany.

Tworzenie profilu zasad

W celu utworzenia profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad. Jeśli zasada nie zawiera profili, pojawi się pusta tabela.

2. Kliknij **Dodaj**.

3. Jeśli chcesz, zmień domyślną nazwę oraz domyślne ustawienia dziedziczenia profilu.

4. Wybierz zakładkę **Ustawienia aplikacji**.

   Lub kliknij **Zapisz** i zakończ działanie. Utworzony profil pojawia się na liście profili zasad i będzie można w późniejszym czasie zmienić ustawienia.

5. Na zakładce **Ustawienia aplikacji**, w lewej części okna wybierz żądaną kategorię, a w prawej części okna zmień ustawienia profilu. Możesz zmienić ustawienia profilu zasad w każdej kategorii (sekcja).

   Podczas edytowania ustawień możesz kliknąć **Anuluj**, aby anulować ostatnie działanie.

6. Kliknij **Zapisz**, aby zapisać profil.

Profil pojawi się na liście profili zasad.

Modyfikowanie profilu zasad

Możliwość modyfikowania profilu zasad jest dostępna tylko dla profili Kaspersky Endpoint Security for Windows.

W celu zmodyfikowania profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** kliknij profil zasady, który chcesz zmodyfikować.

   Zostanie otwarte okno właściwości profilu zasad.

3. Skonfiguruj profil w oknie właściwości:

   - Jeśli to konieczne, na zakładce **Ogólne** zmień nazwę profilu i włącz lub wyłącz profil.
   - Edytuj reguły aktywacji profilu.
   - Edytuj ustawienia aplikacji.

   Szczegółowe informacje dotyczące ustawień aplikacji zabezpieczających można znaleźć w dokumentacji dla odpowiedniej aplikacji.

4. Kliknij **Zapisz**.

Zmodyfikowane ustawienia zostaną zastosowane po zsynchronizowaniu urządzenia z Serwerem administracyjnym (jeśli profil zasad jest aktywny) lub po wyzwoleniu reguły aktywacji (jeśli profil zasad jest nieaktywny).

Kopiowanie profilu zasad

Możesz skopiować profil zasad do bieżącego profilu lub do innego profilu, na przykład, jeśli chcesz mieć identyczne profile dla różnych zasad. Kopiowania możesz użyć także, jeśli chcesz mieć dwa lub więcej profili, które różnią się tylko małą liczbą ustawień.

W celu skopiowania profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad. Jeśli zasada nie zawiera profili, pojawi się pusta tabela.

2. Na zakładce **Profile zasad** wybierz profil zasady, który chcesz skopiować.

3. Kliknij **Kopiuj**.

4. W otwartym oknie wybierz zasadę, do której chcesz skopiować profil.

   Profil zasad możesz skopiować do tego samego profilu lub do profilu, który określiłeś.

5. Kliknij **Kopiuj**.

Profil zasad został skopiowany do wybranego profilu. Nowo skopiowany profil uzyskuje najniższy priorytet. Jeśli skopiujesz profil do tej samej zasady, nazwa nowo skopiowanego profilu zostanie poszerzona o indeks (), na przykład: (1), (2).

Później będziesz mógł zmienić ustawienia profilu, w tym jego nazwę i priorytet; w tym przypadku oryginalny profil zasady nie zostanie zmieniony.

Tworzenie reguły aktywacji profilu zasad

W celu utworzenia reguły aktywacji profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** kliknij profil zasad, dla którego chcesz utworzyć regułę aktywacji.

   Jeśli lista profili zasad jest pusta, możesz utworzyć profil zasad.

3. Na zakładce **Reguły aktywacji** kliknij przycisk **Dodaj**.

   Zostanie otwarte okno z regułami aktywacji profilu zasad.

4. Określ nazwę reguły.

5. Zaznacz pola obok warunków, które mają wpływać na aktywację tworzonego profilu zasad:

   - **Główne reguły dotyczące aktywacji profilu zasad**

     Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od stanu trybu offline urządzenia, regułę połączenia z Serwerem administracyjnym, a także znaczniki przypisywane do urządzenia.

     Dla tej opcji, w następnym kroku określ:

     - **Stan urządzenia**

       Określ warunek obecności urządzenia w sieci:

       - **Online**— Urządzenie jest w sieci, więc Serwer administracyjny jest dostępny.
       - **Offline**— Urządzenie jest w sieci zewnętrznej, co oznacza, że Serwer administracyjny nie jest dostępny.
       - **N/D**—Kryterium nie będzie stosowane.

     - **Reguła dla połączenia Serwera administracyjnego jest aktywna na tym urządzeniu**

       Wybierz warunek aktywacji profilu zasad (czy reguła jest wykonywana) i wybierz nazwę reguły.

       Reguła definiuje lokalizację sieciową urządzenia dla połączenia z Serwerem administracyjnym, którego warunki muszą być spełnione (lub nie muszą być spełnione) dla aktywacji profilu zasad.

       Opis lokalizacji sieciowej urządzeń dla połączenia z Serwerem administracyjnym może zostać utworzony lub skonfigurowany w regule przełączania Agenta sieciowego.

- **Reguły dla określonego właściciela urządzenia**

  Dla tej opcji, w następnym kroku określ:

  - Właściciel urządzenia

    Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu zgodnie z jego właścicielem. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

    - Urządzenie należy do określonego właściciela (znak „=").
    - Urządzenie nie należy do określonego właściciela (znak „#").

      Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić właściciela urządzenia, gdy opcja jest włączona. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

  - Właściciel urządzenia należy do wewnętrznej grupy bezpieczeństwa

    Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według przynależności właściciela do wewnętrznej grupy zabezpieczeń Kaspersky Security Center. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

    - Właściciel urządzenia jest członkiem określonej grupy bezpieczeństwa (znak „=").
    - Właściciel urządzenia nie jest członkiem określonej grupy bezpieczeństwa (znak „#").

      Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić grupę zabezpieczeń Kaspersky Security Center. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- Reguły dla specyfikacji sprzętowej

  Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od ilości pamięci oraz liczby procesów logicznych.

  Dla tej opcji, w następnym kroku określ:

  - Rozmiar pamięci RAM, w MB

    Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu według ilości pamięci RAM dostępnej na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

    - Rozmiar pamięci RAM jest mniejszy niż określona wartość (znak „<").
    - Rozmiar pamięci RAM jest większy niż określona wartość (znak „>").

    Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić ilość pamięci RAM na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

  - Liczba procesorów logicznych

Włącz tę opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu według liczby procesorów logicznych na tym urządzeniu. Z listy rozwijalnej, znajdującej się pod tym polem, możesz wybrać kryterium aktywacji profilu:

- Liczba procesorów logicznych na urządzeniu jest mniejsza niż lub równa określonej wartości (znak „<”).
- Liczba procesorów logicznych na urządzeniu jest większa niż lub równa określonej wartości (znak „>”).

Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium. Możesz określić liczbę procesorów logicznych na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Reguły dla przypisywania roli**

  Dla tej opcji, w następnym kroku określ:

  Aktywuj profil zasad określoną rolą właściciela urządzenia

  Wybierz te opcję, aby skonfigurować i włączyć regułę aktywacji profilu na urządzeniu w zależności od roli właściciela. Dodaj rolę ręcznie z listy istniejących ról.

  Jeśli ta opcja jest włączona, profil zostanie aktywowany na urządzeniu zgodnie ze skonfigurowanym kryterium.

- **Reguły dla użycia znaczników**

  Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od znaczników przypisanych do urządzenia. Możesz aktywować profil zasad dla urządzeń, które posiadają znaczniki lub które ich nie posiadają.

  Dla tej opcji, w następnym kroku określ:

  - **Znacznik**

    Na liście znaczników możesz określić regułę uwzględniania urządzenia w profilu zasad, zaznaczając pola obok odpowiednich znaczników.

    Możesz dodać nowe znaczniki do listy, wprowadzając je w polu nad listą i klikając przycisk **Dodaj**.

    Profil zasad obejmuje urządzenia z opisami zawierającymi wszystkie zaznaczone tagi. Jeśli pola nie są zaznaczone, kryterium nie jest stosowane. Domyślnie pola te nie są zaznaczone.

  - **Zastosuj do urządzeń bez określonych znaczników**

    Włącz tę opcje, jeśli musisz odwrócić wybór znaczników.

    Jeśli ta opcja jest włączona, profil zasad obejmuje urządzenia z opisami, które nie zawierają żadnego z wybranych znaczników. Jeśli ta opcja jest wyłączona, kryterium nie zostanie zastosowane.

    Domyślnie opcja ta jest wyłączona.

- **Reguły dotyczące używania Active Directory**

Zaznacz to pole, aby skonfigurować reguły aktywacji profilu zasad na urządzeniu w zależności od obecności urządzenia w jednostce organizacyjnej Active Directory (OU) lub członkostwa urządzenia (lub jego właściciela) w grupie zabezpieczeń Active Directory.

Dla tej opcji, w następnym kroku określ:

- **Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory**

  Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, którego właściciel jest członkiem określonej grupy zabezpieczeń. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Członkostwo urządzenia w grupie zabezpieczeń Active Directory**

  Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane. Domyślnie opcja ta jest wyłączona.

- **Alokacja urządzenia w jednostce organizacyjnej Active Directory**

  Jeśli ta opcja jest włączona, profil zasad jest aktywowany na urządzeniu, które jest uwzględnione w określonej jednostce organizacyjnej Active Directory. Jeśli ta opcja jest wyłączona, kryterium aktywacji profilu nie jest stosowane.

  Domyślnie opcja ta jest wyłączona.

Liczba dodatkowych okien w kreatorze zależy od ustawień wybranych w pierwszym kroku. Reguły aktywacji profili zasad można zmodyfikować w późniejszym czasie.

6. Sprawdź listę skonfigurowanych parametrów. Jeśli lista jest poprawna, kliknij **Utwórz**.

Profil zostanie zapisany. Profil zostanie aktywowany na urządzeniu po wyzwoleniu reguł aktywacji.

Reguły aktywacji profilu zasad utworzone dla profilu będą wyświetlone we właściwościach profilu zasad, na zakładce **Reguły aktywacji**. Możesz zmodyfikować lub usunąć dowolną regułę aktywacji profilu zasad.

Jednocześnie może być wyzwolonych kilka reguł aktywacji.

Usuwanie profilu zasad

W celu usunięcia profilu zasad:

1. Przejdź do listy profili zasady, której potrzebujesz.

   Zostanie otwarta lista profili zasad.

2. Na zakładce **Profile zasad** zaznacz pole obok profilu zasady, którą chcesz usunąć, a następnie kliknij **Usuń**.

3. W otwartym oknie ponownie kliknij **Usuń**.

Profil zasad został usunięty. Jeśli profil jest dziedziczony przez grupę niskiego poziomu, profil pozostanie w tej grupie, ale stanie się profilem zasady tej grupy. Odbywa się to w celu wyeliminowania znaczących zmian w ustawieniach zarządzanych aplikacji zainstalowanych na urządzeniach grup niskiego poziomu.

Szyfrowanie i ochrona danych

Szyfrowanie danych zmniejsza ryzyko przypadkowego wycieku danych w sytuacji, gdy laptop lub dysk twardy zostanie skradziony lub zgubiony, bądź też, gdy dostęp do danych uzyskują nieautoryzowani użytkownicy lub aplikacje.

Szyfrowanie jest obsługiwane przez następujące aplikacje Kaspersky:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

Za pomocą ustawień interfejsu użytkownika można wyświetlić lub ukryć niektóre elementy interfejsu związane z funkcją zarządzania szyfrowaniem.

Szyfrowanie danych w Kaspersky Endpoint Security for Windows

Możesz zarządzać następującymi typami szyfrowania:

- Szyfrowanie dysków funkcją BitLocker na urządzeniach z systemem operacyjnym Windows dla serwerów
- Kaspersky Disk Encryption na urządzeniach z systemem operacyjnym Windows dla stacji roboczej

Korzystając z tych komponentów Kaspersky Endpoint Security for Windows, możesz na przykład włączyć lub wyłączyć szyfrowanie, przeglądać listę zaszyfrowanych dysków lub generować i przeglądać raporty dotyczące szyfrowania.

Szyfrowanie konfiguruje się, definiując zasady Kaspersky Endpoint Security for Windows w Kaspersky Security Center. Kaspersky Endpoint Security for Windows wykonuje szyfrowanie i deszyfrowanie zgodnie z aktywną zasadą. Szczegółowe instrukcje dotyczące konfigurowania reguł oraz opis funkcji szyfrowania są dostępne w Pomocy Kaspersky Endpoint Security for Windows.

Szyfrowanie danych w Kaspersky Endpoint Security for Mac

Możesz użyć szyfrowania FileVault na urządzeniach z systemem macOS. Podczas pracy z Kaspersky Endpoint Security for Mac możesz włączyć lub wyłączyć to szyfrowanie.

Szyfrowanie konfiguruje się, definiując zasady Kaspersky Endpoint Security for Mac w Kaspersky Security Center. Kaspersky Endpoint Security for Mac wykonuje szyfrowanie i deszyfrowanie zgodnie z aktywną zasadą. Szczegółowy opis funkcji szyfrowania znajduje się w Pomocy Kaspersky Endpoint Security for Mac.

Przeglądanie listy zaszyfrowanych dysków

W Kaspersky Security Center możesz przeglądać szczegółowe informacje o zaszyfrowanych dyskach i urządzeniach zaszyfrowanych na poziomie dysku. Po odszyfrowaniu informacji na dysku, dysk jest automatycznie usuwane z listy.

W celu przejrzenia listy zaszyfrowanych dysków:

W menu głównym przejdź do **Operacje → Szyfrowanie i ochrona danych → Zaszyfrowane dyski**.

Jeśli sekcji nie ma w menu, oznacza to, że jest ukryta. W ustawieniach interfejsu użytkownika włącz opcję **Pokaż szyfrowanie i ochronę danych**, aby wyświetlić sekcję.

Możesz wyeksportować listę zaszyfrowanych dysków do pliku CSV lub pliku TXT. W tym celu kliknij przycisk **Eksportuj wiersze do pliku CSV** lub **Eksportuj wiersze do pliku TXT**.

Wyświetlanie listy zdarzeń szyfrowania

Podczas wykonywania zadań szyfrowania lub deszyfrowania danych na urządzeniach, Kaspersky Endpoint Security for Windows wysyła do Kaspersky Security Center informacje o zdarzeniach następujących typów:

- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak wolnego miejsca na dysku.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na problemy z licencją.
- Nie można zaszyfrować ani odszyfrować pliku lub utworzyć zaszyfrowanego archiwum ze względu na brak praw dostępu.
- Dla aplikacji zablokowano dostęp do zaszyfrowanego pliku.
- Nieznane błędy.

W celu wyświetlenia listy zdarzeń, które wystąpiły w trakcie szyfrowania danych na urządzeniach:

W menu głównym przejdź do **Operacje → Szyfrowanie i ochrona danych → Zdarzenia szyfrowania**.

Jeśli sekcji nie ma w menu, oznacza to, że jest ukryta. W ustawieniach interfejsu użytkownika włącz opcję **Pokaż szyfrowanie i ochronę danych**, aby wyświetlić sekcję.

Możesz wyeksportować listę zaszyfrowanych dysków do pliku CSV lub pliku TXT. W tym celu kliknij przycisk **Eksportuj wiersze do pliku CSV** lub **Eksportuj wiersze do pliku TXT**.

Alternatywnie możesz przejrzeć listę zdarzeń szyfrowania dla każdego zarządzanego urządzenia.

Aby wyświetlić zdarzenia szyfrowania dla zarządzanego urządzenia:

1. W menu głównym przejdź do **Urządzenia → Zarządzane urządzenia**.
2. Kliknij nazwę zarządzanego urządzenia.
3. Na karcie **Ogólne** przejdź do sekcji **Ochrona**.
4. Kliknij łącze **Wyświetl błędy szyfrowania danych**.

Tworzenie i przeglądanie raportów z szyfrowania

Możesz wygenerować następujące raporty:

- Raport o stanie szyfrowania zarządzanych urządzeń. Ten raport zawiera szczegółowe informacje na temat szyfrowania danych na różnych zarządzanych urządzeniach. Na przykład raport pokazuje liczbę urządzeń, do których ma zastosowanie polityka ze skonfigurowanymi regułami szyfrowania. Możesz także dowiedzieć się, na przykład, ile urządzeń wymaga ponownego uruchomienia. Raport zawiera również informacje o technologii i algorytmie szyfrowania dla każdego urządzenia.

- Raport o stanie szyfrowania urządzeń pamięci masowej. Ten raport zawiera podobne informacje jak raport o stanie szyfrowania zarządzanych urządzeń, ale zawiera dane tylko dla urządzeń pamięci masowej i dysków wymiennych.

- Raport o prawach dostępu do zaszyfrowanych dysków. Ten raport pokazuje, które konta użytkowników mają dostęp do zaszyfrowanych dysków.

- Raport o błędach podczas szyfrowania plików. Ten raport zawiera informacje o błędach, które wystąpiły podczas uruchamiania zadań szyfrowania lub deszyfrowania danych na urządzeniach.

- Raport o zablokowanym dostępie do zaszyfrowanych plików. Ten raport zawiera informacje o blokowaniu dostępu aplikacji do zaszyfrowanych plików. Ten raport jest pomocny, jeśli nieautoryzowany użytkownik lub aplikacja próbuje uzyskać dostęp do zaszyfrowanych plików lub dysków.

Możesz wygenerować dowolny raport w sekcji **Monitorowanie i raportowanie** → **Raporty**). Alternatywnie w sekcji **Operacje** → **Szyfrowanie i ochrona danych** możesz wygenerować następujące raporty dotyczące szyfrowania:

- Raport o stanie szyfrowania urządzeń pamięci masowej
- Raport o prawach dostępu do zaszyfrowanych dysków
- Raport o błędach podczas szyfrowania plików

*Aby wygenerować raport szyfrowania w sekcji **Szyfrowanie i ochrona danych**:*

1. Upewnij się, że włączyłeś opcję **Pokaż szyfrowanie i ochronę danych** w opcjach interfejsu.
2. W menu głównym przejdź do **Operacje** → **Szyfrowanie i ochrona danych**.
3. Wybierz jedną z następujących sekcji:
   - **Zaszyfrowane dyski** generuje raport o stanie szyfrowania urządzeń pamięci masowej lub raport o prawach dostępu do zaszyfrowanych dysków.
   - **Zdarzenia szyfrowania** generuje raport o błędach szyfrowania plików.
4. Kliknij nazwę raportu, który chcesz wygenerować.

Zostanie rozpoczęte tworzenie raportu.

Udzielanie dostępu do zaszyfrowanego dysku w trybie offline

Użytkownik może poprosić o dostęp do zaszyfrowanego urządzenia, na przykład, gdy Kaspersky Endpoint Security for Windows nie jest zainstalowany na zarządzanym urządzeniu. Po otrzymaniu żądania możesz utworzyć plik klucza dostępu i wysłać go do użytkownika. Wszystkie przypadki użycia i szczegółowe instrukcje znajdują się w Pomocy Kaspersky Endpoint Security for Windows.

W celu udzielenia dostępu do zaszyfrowanego dysku w trybie offline:

1. Uzyskaj plik żądania dostępu od użytkownika (plik z rozszerzeniem FDERTC). Postępuj zgodnie z instrukcjami zawartymi w Pomocy Kaspersky Endpoint Security for Windows aby wygenerować plik w Kaspersky Endpoint Security for Windows.
2. W menu głównym przejdź do **Operacje → Szyfrowanie i ochrona danych → Zaszyfrowane dyski**.

   Zostanie wyświetlona lista zaszyfrowanych dysków.
3. Wybierz dysk, do którego użytkownik zażądał dostępu.
4. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.
5. W oknie, które zostanie otwarte, wybierz wtyczkę odpowiadającą aplikacji Kaspersky, która została użyta do zaszyfrowania wybranego dysku.

   Jeśli dysk jest zaszyfrowany przy pomocy aplikacji Kaspersky, która nie jest obsługiwana przez konsolę Kaspersky Security Center Web Console, użyj Konsoli administracyjnej opartej na Microsoft Management Console, aby udzielić dostępu offline.
6. Postępuj zgodnie z instrukcjami podanymi w Pomocy Kaspersky Endpoint Security for Windows (patrz rozwijające się bloki na końcu sekcji).

Po zakończeniu użytkownik stosuje otrzymany plik, aby uzyskać dostęp do zaszyfrowanego dysku i odczytać dane zapisane na dysku.

Użytkownicy i role użytkownika

Ta sekcja opisuje użytkowników i role użytkownika, a także zawiera instrukcje ich tworzenia i modyfikowania, przydzielania ról i grup do użytkowników, a także kojarzenia profili zasad z rolami.

Informacje o rolach użytkowników

Rola użytkownika (zwana dalej *rolą*) to obiekt zawierający zestaw praw i uprawnień. Rola może zostać skojarzona z ustawieniami aplikacji Kaspersky zainstalowanych na urządzeniu użytkownika. Możesz przypisać rolę do zestawu użytkowników lub do zestawu grup bezpieczeństwa na dowolnym poziomie w hierarchii grup administracyjnych, Serwerów administracyjnych lub na poziomie określonych obiektów.

Jeśli zarządzasz urządzeniami poprzez hierarchię Serwerów administracyjnych, która obejmuje wirtualne Serwery administracyjne, pamiętaj, że możesz tworzyć, modyfikować lub usuwać role użytkowników tylko z fizycznego Serwera administracyjnego. Następnie możesz propagować role użytkowników na drugorzędne Serwery administracyjne, w tym wirtualne.

Możesz skojarzyć role użytkownika z profilami zasad. Jeśli użytkownikowi przydzielono rolę, ten użytkownik uzyska ustawienia zabezpieczeń niezbędne do pełnienia funkcji związanych z jego stanowiskiem pracy.

Rola użytkownika może zostać skojarzona z użytkownikami urządzeń w określonej grupie administracyjnej.

Obszar roli użytkownika

Obszar roli użytkownika to połączenie użytkowników i grup administracyjnych. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup potomnych.

Korzyści korzystania z ról

Korzyścią korzystania z ról jest brak konieczności określenia ustawień zabezpieczeń dla każdego z zarządzanych urządzeń lub dla każdego z użytkowników oddzielnie. Liczba użytkowników i urządzeń w firmie może być całkiem duża, ale liczba różnych stanowisk pracy, które wymagają różnych ustawień zabezpieczeń jest znacząco mała.

Różnice wynikające z używania profili zasad

Profile zasad to właściwości zasady tworzone dla każdej aplikacji Kaspersky oddzielnie. Rola jest skojarzona z wieloma profilami zasad utworzonymi dla różnych aplikacji. Dlatego też rola jest metodą zebrania ustawień dla określonego typu użytkownika w jednym miejscu.

Konfigurowanie praw dostępu do funkcji aplikacji. Kontrola dostępu oparta o rolę

Kaspersky Security Center oferuje możliwości dla dostępu opartego na roli do funkcji Kaspersky Security Center i zarządzanych aplikacji firmy Kaspersky.

Możesz skonfigurować uprawnienia dostępu do funkcji aplikacji dla użytkowników Kaspersky Security Center w jeden z następujących sposobów:

- Konfigurując uprawnienia dla każdego użytkownika lub grupy użytkowników indywidualnie.
- Tworząc standardowe role użytkownika z predefiniowanym zestawem uprawnień i przypisując te role do użytkowników w zależności od ich zakresu obowiązków.

Stosowanie ról użytkownika jest przeznaczone do uproszczenia i skrócenia rutynowych procedur konfigurowania uprawnień dostępu użytkowników do funkcji aplikacji. Uprawnienia dostępu w obrębie roli są konfigurowane zgodnie ze 'standardowymi' zadaniami i zakresem obowiązków użytkowników.

Rolom użytkownika można przypisać nazwy, które odpowiadają ich przeznaczeniu. Możesz utworzyć nieograniczoną liczbę ról.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role i samodzielnie skonfigurować wymagane uprawnienia.

Prawa dostępu do funkcji aplikacji

Poniższa tabela przedstawia funkcje Kaspersky Security Center wraz z prawami dostępu do zarządzania powiązanymi zadaniami, raportami, ustawieniami i wykonywania powiązanych działań użytkownika.

Aby wykonać czynności użytkownika wymienione w tabeli, użytkownik musi mieć określone uprawnienia obok akcji.

Prawa do **odczytu**, **wpisywania** i **wykonywania** mają zastosowanie do każdego zadania, raportu lub ustawienia. Oprócz tych praw użytkownik musi mieć uprawnienie **Wykonaj operacje na wyborach urządzeń**, aby zarządzać zadaniami, raportami lub ustawieniami wyborów urządzeń.

Wszystkie zadania, raporty, ustawienia i pakiety instalacyjne, których brakuje w tabeli, należą do obszaru funkcjonalnego **Funkcje ogólne: Podstawowa funkcjonalność**.

Prawa dostępu do funkcji aplikacji

Obszar funkcjonalny	Uprawnienie	Akcja użytkownika: uprawnienia wymagane do wykonania akcji	Zadanie	Raport
Funkcje ogólne: **Zarządzanie grupami administracyjnymi**	**Wpisz**	• Dodaj urządzenie do grupy administracyjnej: **Wpisz** • Usuń urządzenie z grupy administracyjnej: **Wpisz** • Dodaj grupę administracyjną do innej grupy administracyjnej: **Wpisz** • Usuń grupę administracyjną z innej grupy administracyjnej: **Wpisz**	Brak	Brak
Funkcje ogólne: **Uzyskuj dostęp do obiektów bez względu na ich listy ACL**	**Odczyt**	Uzyskaj dostęp do odczytu do wszystkich obiektów: **Odczyt**	Brak	Brak
Cechy ogólne: Podstawowa funkcjonalność	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Reguły przenoszenia urządzeń (tworzenie, modyfikowanie lub usuwanie) dla Serwera wirtualnego: **Wpisz**, **Wykonuj** operacje na	• „Pobierz aktualizacje do repozytorium serwera administracyjnego” • „Dostarczaj raporty” • „Roześlij pakiet instalacyjny”	• „Raport o sta ochrony” • „Raport o zagrożeniach” • „Raport o najbardziej zainfekowany urządzeniach”

		wybranych urządzeniach • Uzyskaj niestandardowy certyfikat protokołu Mobile (LWNGT): **Odczytaj** • Ustaw certyfikat niestandardowy protokołu Mobile (LWNGT): **Zapisz** • Uzyskaj listę sieci zdefiniowaną przez NLA: **Odczytaj** • Dodaj, zmodyfikuj lub usuń listę sieci zdefiniowaną przez NLA: **Wpisz** • Wyświetl listę kontroli dostępu grup: **Odczytaj** • Wyświetl dziennik zdarzeń aplikacji Kaspersky: **Odczytaj**	• „Zdalnie zainstaluj aplikację na podrzędnych Serwerach administracyjnych”	• „Raport o sta antywirusowy baz danych” • „Raport o błędach” • „Raport o ata sieciowych” • „Raport podsumowuja na temat zainstalowany aplikacji chroniących system poczt • „Raport podsumowuja na temat zainstalowany aplikacji ochro obwodowej” • „Raport podsumowuja na temat typo zainstalowany aplikacji” • „Raport o użytkownikac zainfekowany urządzeń” • „Raport incydentów” • „Raport wyda • „Raport o aktywności punktów dystrybucji” • „Raport o podrzędnych Serwerach administracyj • „Raport zdarz Kontroli urząc • „Raport o luka • „Raport o zabronionych

				aplikacjach" • „Raport Kontr sieci" • „Raport o sta szyfrowania zarządzanych urządzeń" • „Raport o sta szyfrowania urządzeń pam masowej" • „Raport o błę podczas szyfrowania plików" • „Raport o zablokowanyr dostępie do zaszyfrowany plików" • „Raport o uprawnieniacl dostępu do zaszyfrowany urządzeń" • „Raport o efektywnych uprawnieniacl użytkowników • „Raport dotyc uprawnień"
Funkcje ogólne: **Obiekty usunięte**	• **Odczyt** • **Wpisz**	• Wyświetl usunięte obiekty w Koszu: **Odczytaj** • Usuń obiekty z Kosza: **Wpisz**	Brak	Brak
Funkcje ogólne: **Przetwarzanie zdarzeń**	• **Usuń zdarzenia** • **Edytuj ustawienia powiadomień o zdarzeniach** • **Edytuj ustawienia rejestrowania zdarzeń**	• Zmień ustawienia rejestracji zdarzeń: **Edytuj ustawienia rejestrowania zdarzeń** • Zmień ustawienia powiadomień o zdarzeniach:	Brak	Brak

	• **Wpisz**	**Edytuj ustawienia powiadomień o zdarzeniach** • Usuń zdarzenia: **Usuń zdarzenia**		
Funkcje ogólne: **Operacje na Serwerze administracyjnym**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Modyfikuj listy ACL obiektów** • **Wykonaj operacje na wyborach urządzeń**	• Określ porty Serwera administracyjnego dla połączenia agenta sieciowego: **Wpisz** • Określ porty Serwera proxy aktywacji uruchomionego na serwerze administracyjnym Serwer administracyjny: **Wpisz** • Określ porty serwera proxy aktywacji dla urządzeń przenośnych uruchomionych na Serwerze administracyjnym: **Wpisz** • Określ porty serwera sieciowego do dystrybucji samodzielnych pakietów: **Wpisz** • Określ porty serwera sieciowego do dystrybucji profili MDM: **Wpisz** • Określ porty SSL Serwera	• „Tworzenie kopii zapasowych danych Serwera administracyjnego" • „Konserwacja baz danych"	Brak

		administracyjnego do połączenia przez Kaspersky Security Center Web Console: **Wpisz** • Określ porty serwera administracyjnego Serwer administracyjny dla połączenia mobilnego: **Wpisz** • Zmienianie maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego: **Wpisz** • Określ maksymalną liczbę zdarzeń, które mogą być wysłane przez Serwer administracyjny: **Wpisz** • Określ przedział czasu, w którym zdarzenia mogą być wysyłane przez Serwer administracyjny: **Wpisz**		
Funkcje ogólne: **Wdrażanie oprogramowania Kaspersky**	• **Zarządzaj poprawkami Kaspersky** • **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	Zaakceptuj lub odrzuć instalację poprawki: **Zarządzaj poprawkami Kaspersky**	Brak	• „Raport dotyc użycia klucza licencyjnego p wirtualny serv administracyj • „Raport o wersjach oprogramowa Kaspersky” • „Raport o niekompatybi aplikacjach” • „Raport o wersjach aktualizacji

				modułu oprogramowa Kaspersky" • „Raport wdra ochrony"
Cechy ogólne: **Zarządzanie kluczami**	• **Eksportuj plik klucza** • **Wpisz**	• Eksportuj plik klucza: **Eksportuj plik klucza** • Zmodyfikuj ustawienia klucza licencyjnego Serwera administracyjnego: **Wpisz**	Brak	Brak
Funkcje ogólne: **Wymuszone zarządzanie raportami**	• **Odczyt** • **Wpisz**	• Twórz raporty niezależnie od ich list ACL: **Zapisz** • Wykonywanie raportów niezależnie od ich list ACL: **Odczytaj**	Brak	Brak
Funkcje ogólne: **Hierarchia serwerów administracyjnych**	**Skonfiguruj hierarchię Serwerów administracyjnych**	Zarejestruj, zaktualizuj lub usuń podrzędne Serwery administracyjne: **Skonfiguruj hierarchię Serwerów administracyjnych**	Brak	Brak
Cechy ogólne: **Uprawnienia użytkownika**	**Modyfikuj listy ACL obiektów**	• Zmień właściwości Zabezpieczenia dowolnego obiektu: **Modyfikuj listy ACL obiektów** • Zarządzaj rolami użytkowników: **Modyfikuj listy ACL obiektów** • Zarządzaj użytkownikami wewnętrznymi: **Modyfikuj listy ACL obiektów** • Zarządzaj grupami zabezpieczeń:	Brak	Brak

		Modyfikuj listy ACL obiektów • Zarządzaj aliasami: **Modyfikuj listy ACL obiektów**		
Funkcje ogólne: **Wirtualne serwery administracyjne**	• **Zarządzaj wirtualnym serwerem administracyjnym Serwery administracyjne** • **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Pobierz listę wirtualnych serwerów administracyjnych Serwery administracyjne: **Odczytaj** • Uzyskaj informacje na temat wirtualnego Serwera administracyjnego: **Odczytaj** • Utwórz, zaktualizuj lub usuń wirtualny Serwer administracyjny: **Zarządzaj wirtualnymi serwerami administracyjnymi** • Przenieś wirtualny Serwer administracyjny do innej grupy: **Zarządzaj wirtualnymi serwerami administracyjnymi** • Ustaw uprawnienia do administracyjnego Serwera wirtualnego: **Zarządzaj wirtualnymi serwerami administracyjnymi**	Brak	„Raport o wynika instalacji aktualiz oprogramowania trzecich”
Funkcje ogólne: **Zarządzanie kluczami szyfrowania**	**Wpisz**	Zaimportuj klucze szyfrowania: **Wpisz**	Brak	Brak
Zarządzanie urządzeniami	• **Podłączanie nowych urządzeń**	• Uzyskaj dane przywracania	Brak	Brak

mobilnymi: Ogólne	• **Wysyłaj tylko polecenia informacyjne na urządzenia mobilne** • **Wysyłanie poleceń na urządzenia mobilne** • **Zarządzaj certyfikatami** • **Odczyt** • **Wpisz**	Usługi zarządzania kluczami: **Odczytaj** • Usuń certyfikaty użytkownika: **Zarządzaj certyfikatami** • Uzyskaj część publiczną certyfikatu użytkownika: **Odczytaj** • Sprawdź, czy infrastruktura klucza publicznego jest włączona: **Odczytaj** • Sprawdź konto infrastruktury klucza publicznego: **Odczytaj** • Uzyskaj szablony infrastruktury klucza publicznego: **Odczytaj** • Uzyskaj szablony infrastruktury klucza publicznego za pomocą certyfikatu rozszerzonego użycia klucza: **Odczytaj** • Sprawdź, czy certyfikat infrastruktury klucza publicznego został odwołany: **Odczytaj** • Zaktualizuj ustawienia wydawania certyfikatów użytkownika: **Zarządzaj certyfikatami** • Uzyskaj ustawienia wydawania certyfikatu	

		użytkownika: **Odczytaj** • Pobierz pakiety według nazwy i wersji aplikacji: **Odczytaj** • Ustaw lub anuluj certyfikat użytkownika: **Zarządzaj certyfikatami** • Odnów certyfikat użytkownika: **Zarządzaj certyfikatami** • Ustaw tag certyfikatu użytkownika: **Zarządzaj certyfikatami** • Uruchom generację pakietu instalacyjnego MDM; anuluj generowanie pakietu instalacyjnego MDM: **Podłącz nowe urządzenia**		
Zarządzanie systemem: **Łączność**	• **Rozpocznij sesje RDP** • **Połącz się z istniejącymi sesjami RDP** • **Rozpocznij tunelowanie** • **Zapisz pliki z urządzeń na stacji roboczej administratora** • **Odczyt** • **Wpisz** • **Wykonaj**	• Utwórz sesję udostępniania pulpitu: **Prawo do tworzenia sesji udostępniania pulpitu** • Utwórz sesję RDP: **Połącz się z istniejącymi sesjami RDP** • Utwórz tunel: **Zainicjuj tunelowanie** • Zapisz listę sieci partnerskiej: **Zapisz pliki z urządzeń na stacji roboczej administratora**	Brak	„Raport o użytkownikach urządzenia”

	• **Wykonaj operacje na wyborach urządzeń**			
Zarządzanie systemem: **Inwentaryzacja sprzętu**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Pobierz lub wyeksportuj obiekt spisu sprzętu: **Odczytaj** • Dodaj, ustaw lub usuń obiekt spisu sprzętu: **Zapisz**	Brak	• „Raport rejest sprzętu" • „Raport o zmianach konfiguracji" • „Raport o sprzęcie"
Zarządzanie systemem: **Kontrola dostępu do sieci**	• **Odczyt** • **Wpisz**	• Wyświetl ustawienia CISCO: **Odczytaj** • Zmień ustawienia CISCO: **Zapisz**	Brak	Brak
Zarządzanie systemem: **Wdrażanie systemu operacyjnego**	• **Instalowanie serwerów PXE** • **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Zainstaluj serwer PXE: **Instalowanie serwerów PXE** • Wyświetl listę serwerów PXE: **Odczytaj** • Rozpocznij lub zatrzymaj proces instalacji na klientach PXE: **Wykonaj** • Zarządzaj sterownikami dla WinPE i obrazów systemu operacyjnego: **Wpisz**	„Utwórz pakiet instalacyjny na podstawie obrazu systemu operacyjnego urządzenia odniesienia"	Brak
Zarządzanie systemem: **zarządzanie lukami i poprawkami**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Wyświetl właściwości poprawki trzeciej firmy: **Odczytaj** • Zmień właściwości poprawki trzeciej firmy: **Wpisz**	• „Wykonać synchronizację Windows Update" • „Instalacja aktualizacji Windows Update" • „Napraw luki"	„Raport o aktualizacjach oprogramowania

			• „Zainstaluj wymagane aktualizacje i napraw luki”	
Zarządzanie systemem: **Zdalna instalacja**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Przejrzyj właściwości pakietu instalacyjnego Zarządzanie lukami i poprawkami innych firm: **Odczytaj** • Zmień właściwości pakietu instalacyjnego Zarządzanie lukami i poprawkami innych firm: **Wpisz**	Brak	Brak
Zarządzanie systemem: **Inwentaryzacja oprogramowania**	• **Odczyt** • **Wpisz** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	Brak	Brak	• „Raport o zainstalowany aplikacjach” • „Raport o rejestrze aplik • „Raport o sta grup licencjonowar aplikacji” • „Raport dotyc kluczy licencyjnych oprogramowa innych firm”

Informacje o rolach użytkowników

Role użytkowników przypisane do użytkowników Kaspersky Security Center zapewniają im zestawy praw dostępu do funkcji aplikacji.

Możesz użyć predefiniowanych ról użytkownika z już skonfigurowanym zestawem uprawnień lub utworzyć nowe role i samodzielnie skonfigurować wymagane uprawnienia. Niektóre z predefiniowanych ról użytkowników dostępnych w Kaspersky Security Center mogą być powiązane z określonymi stanowiskami pracy, na przykład **Audytor**, **Specjalista ds. zabezpieczeń**, **Opiekun** (te role są obecne w Kaspersky Security Center od wersji 11). Prawa dostępu do tych ról są wstępnie skonfigurowane zgodnie ze standardowymi zadaniami i zakresem obowiązków powiązanych stanowisk. Poniższa tabela pokazuje jak role mogą zostać powiązane z określonymi stanowiskami pracy:

Przykłady ról dla określonych stanowisk pracy

Rola	Komentarz
Audytor	Zezwala na wszystkie działania na wszystkich typach raportów, na wszystkie działania przeglądania, w tym przeglądanie usuniętych obiektów (nadaje uprawnienia **Odczyt** i **Zapisz** w obszarze **Usunięte obiekty**). Nie zezwala na pozostałe działania. Tę rolę można przypisać do osoby, która przeprowadza audyt w Twojej organizacji.
Opiekun	Zezwala na wszystkie działania przeglądania, ale nie zezwala na pozostałe działania. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Specjalista ds. zabezpieczeń	Zezwala na wszystkie działania przeglądania, zezwala na zarządzanie raportami; przydziela ograniczone uprawnienia w obszarze **Zarządzanie systemami**: **Łączność**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.

Poniższa tabela przedstawia prawa dostępu przypisane do każdej predefiniowanej roli użytkownika.

Prawa dostępu do predefiniowanych ról użytkowników

Rola	Opis

Administrator serwera administracyjnego	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Przetwarzanie zdarzeń**
	  • **Hierarchia Serwerów administracyjnych**
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie systemami**:
	  • **Łączność**
	  • **Inwentaryzacja sprzętu**
	  • **Inwentaryzacja oprogramowania**
	Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.

Operator serwera administracyjnego	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie systemami**:
	  • **Łączność**
	  • **Inwentaryzacja sprzętu**
	  • **Inwentaryzacja oprogramowania**

Audytor	Zezwala na wszystkie operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Usunięte obiekty** • **Wymuszone zarządzanie raportami** Tę rolę można przypisać do osoby, która przeprowadza audyt w Twojej organizacji.

Administrator instalacji	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Zdalna instalacja oprogramowania Kaspersky**
	  • **Zarządzanie kluczami licencyjnymi**
	• **Zarządzanie systemami**:
	  • **Nazwa systemu operacyjnego**
	  • **Zarządzanie lukami i poprawkami**
	  • **Instalacja zdalna**
	  • **Inwentaryzacja oprogramowania**
	Przyznaje uprawnienia do **odczytu** i **wykonywania** w obszarze funkcjonalnym **Funkcje ogólne: Wirtualne serwery administracyjne**.

Operator instalacji	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Zdalna instalacja oprogramowania Kaspersky** (zapewnia również **Zarządzanie poprawkami Kaspersky** bezpośrednio w tym obszarze)
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie systemami**:
	  • **Nazwa systemu operacyjnego**
	  • **Zarządzanie lukami i poprawkami**
	  • **Instalacja zdalna**
	  • **Inwentaryzacja oprogramowania**

Administrator Kaspersky	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność**

Endpoint Security	• Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.
Operator Kaspersky Endpoint Security	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
Główny administrator	Zezwala na wszystkie operacje w obszarach funkcjonalnych, z *wyjątkiem* następujących obszarów w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami** Przyznaje uprawnienia do **Odczytu** i **Wpisania** w obszarze **Funkcje ogólne: obszar funkcjonalny zarządzania kluczami szyfrowania**.

Główny operator	Przyznaje prawa **odczytu** i **wykonywania** (w stosownych przypadkach) we wszystkich następujących obszarach funkcjonalnych:
	• **Funkcje ogólne**:
	  • **Podstawowa funkcjonalność**
	  • **Usunięte obiekty**
	  • **Operacje na Serwerze administracyjnym**
	  • **Wdrażanie oprogramowania Kaspersky**
	  • **Wirtualne Serwery administracyjne**
	• **Zarządzanie urządzeniami mobilnymi: ogólne**
	• **Zarządzanie systemem**, w tym wszystkie funkcje
	• Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje

Administrator zarządzania urządzeniami mobilnymi	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • **Zarządzanie urządzeniami mobilnymi: ogólne**
Operator zarządzania urządzeniami mobilnymi	Przyznaje uprawnienia **Odczyt** i **Wykonywanie** w obszarze funkcjonalnym **Funkcje ogólne**: **Podstawowa funkcjonalność**. Przyznaje uprawnienia **odczytu** i **wysyłania** informacji poleceń na urządzenia mobilne w obszarach funkcjonalnych **Zarządzania urządzeniami mobilnymi**: **Ogólne**.
Specjalista ds. zabezpieczeń	Zezwala na następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Uzyskuj dostęp do obiektów bez względu na ich listy ACL** • **Wymuszone zarządzanie raportami**

	Przyznaje uprawnienia **Odczytu**, **Wpisania**, **Wykonywania**, **Zapisywania** plików z urządzeń na stacji roboczej administratora i **wykonywania działań dla wyborów urządzeń w obszarze funkcjonalnym Zarządzanie systemami: Łączność**. Możesz przypisać tę rolę do specjalisty zarządzającego bezpieczeństwem IT w Twojej firmie.
Użytkownik portalu Self Service Portal	Zezwala na wszystkie operacje w obszarze funkcjonalnym **Zarządzanie urządzeniami mobilnymi: Self Service Portal**. Ta funkcja nie jest obsługiwana w Kaspersky Security Center 11 i nowszej wersji.
Opiekun	Przyznaje prawo do **Odczytu** w obszarach funkcjonalnych **Funkcje ogólne**: **Dostęp do obiektów, niezależnie od ich list ACL** i **Funkcje ogólne**: **Wymuszone zarządzanie raportami**. Możesz przypisać tę rolę do specjalisty ds. zabezpieczeń i innych menadżerów zarządzających bezpieczeństwem IT w Twojej firmie.
Administrator zarządzania lukami i poprawkami	Zezwala na wszystkie operacje w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje).
Operator zarządzania lukami i poprawkami	Przyznaje uprawnienia **Odczyt** i **Wykonywanie** (w stosownych przypadkach) w obszarach funkcjonalnych **Funkcje ogólne**: **Podstawowa funkcjonalność** i **Zarządzanie systemem** (w tym wszystkie funkcje).

Nadawanie praw dostępu do określonych obiektów

Oprócz nadawania praw dostępu na poziomie serwera, możesz skonfigurować dostęp do konkretnych obiektów, np. do konkretnego zadania. Aplikacja umożliwia określenie praw dostępu do następujących typów obiektów:

- Grupy administracyjne
- Zadania
- Raporty
- Wybory urządzeń
- Wybory zdarzeń

Aby przypisać prawa dostępu do określonego obiektu:

1. W zależności od typu obiektu, w menu głównym przejdź do odpowiedniej sekcji:
   - **Urządzenia → Hierarchia grup**
   - **Urządzenia → Zadania**
   - **Monitorowanie i raportowanie → Raporty**
   - **Urządzenia → Wybory urządzeń** URZĄDZEŃ
   - **Monitorowanie i raportowanie → Wybory zdarzeń**

2. Otwórz właściwości obiektu, do którego chcesz skonfigurować prawa dostępu.

   Aby otworzyć okno właściwości grupy administracyjnej lub zadania, kliknij nazwę obiektu. Właściwości innych obiektów można otworzyć za pomocą przycisku na pasku narzędzi.

3. W oknie właściwości otwórz sekcję **Prawa dostępu**.

   Zostanie otwarta lista użytkowników. Wymienieni użytkownicy i podane grupy zabezpieczeń mają prawa dostępu do obiektu. Domyślnie, jeśli używasz hierarchii grup administracyjnych lub Serwerów, lista i prawa dostępu są dziedziczone z nadrzędnej grupy administracyjnej lub Serwera podstawowego.

4. Aby móc modyfikować listę, włącz opcję **Użyj uprawnień niestandardowych**.

5. Skonfiguruj prawa dostępu:

   - Użyj przycisków **Dodaj** i **Usuń**, aby zmodyfikować listę.
   - Określ prawa dostępu dla użytkownika lub grupy zabezpieczeń. Wykonaj jedną z poniższych czynności:
     - Jeśli chcesz ręcznie określić prawa dostępu, wybierz użytkownika lub grupę zabezpieczeń, kliknij przycisk **Prawa dostępu**, a następnie określ prawa dostępu.
     - Jeśli chcesz przypisać rolę użytkownika do użytkownika lub grupy zabezpieczeń, wybierz użytkownika lub grupę zabezpieczeń, kliknij przycisk **Role**, a następnie wybierz rolę do przypisania.

6. Kliknij przycisk **Zapisz**.

Prawa dostępu do obiektu zostały skonfigurowane.

Dodawanie konta użytkownika wewnętrznego

W celu dodania nowego konta użytkownika wewnętrznego do Kaspersky Security Center:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij **Dodaj**.
3. W otwartym oknie **Nowa jednostka** określ ustawienia nowego konta użytkownika:
   - Zachowaj domyślną opcję **Użytkownik**.
   - **Nazwa**.
   - **Hasło** dla połączenia użytkownika z Kaspersky Security Center.
     Hasło musi być zgodne z następującymi regułami:
     - Hasło musi zawierać od 8 do 16 znaków.
     - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
       - Wielkie litery (A-Z)
       - Małe litery (a-z)

- Cyfry (0-9)
- Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

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

Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

> Liczba prób wprowadzenia hasła jest ograniczona. Domyślnie jest to 10 prób. Możesz zmienić dozwoloną liczbę prób wprowadzenia hasła, jak opisano to w sekcji „Zmienianie liczby dozwolonych prób wprowadzenia hasła”.

> Jeśli użytkownik wprowadzi nieprawidłowe hasło określoną liczbę razy, konto użytkownika zostanie zablokowane na jedną godzinę. Możesz odblokować konto użytkownika tylko poprzez zmianę hasła.

- **Pełna nazwa**
- **Opis**
- **Adres e-mail**
- **Telefon**

4. Kliknij **OK**, aby zachować zmiany.

Nowe konto użytkownika pojawi się na liście użytkowników i grup użytkowników.

Tworzenie grupy użytkowników

W celu utworzenia grupy użytkowników:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij **Dodaj**.
3. W otwartym oknie **Nowa jednostka** wybierz **Grupa**.
4. Określ następujące ustawienia dla nowej grupy użytkowników:
   - **Nazwa grupy**
   - **Opis**
5. Kliknij **OK**, aby zachować zmiany.

Nowa grupa użytkowników pojawi się na liście użytkowników i grup użytkowników.

Edytowanie konta użytkownika wewnętrznego

W celu edytowania konta użytkownika wewnętrznego w Kaspersky Security Center:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij nazwę konta użytkowników, które chcesz edytować.
3. W otwartym oknie ustawień użytkownika, na zakładce **Ogólne** zmień ustawienia konta użytkownika:
   - **Opis**
   - **Pełna nazwa**
   - **Adres e-mail**
   - **Główny numer telefonu**
   - **Hasło** dla połączenia użytkownika z Kaspersky Security Center.
     Hasło musi być zgodne z następującymi regułami:
     - Hasło musi zawierać od 8 do 16 znaków.
     - Hasło musi zawierać znaki z przynajmniej trzech z poniższych grup:
       - Wielkie litery (A-Z)
       - Małe litery (a-z)
       - Cyfry (0-9)
       - Znaki specjalne (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - Hasło nie może zawierać spacji, znaków Unicode lub kombinacji znaków "." i "@", gdy "." jest umieszczane przed "@".

     Aby zobaczyć wprowadzone hasło, kliknij i przytrzymaj przycisk **Pokaż**.

     > Liczba prób wprowadzenia hasła jest ograniczona. Domyślnie jest to 10 prób. Możesz zmienić dozwoloną liczbę prób; jednak ze względów bezpieczeństwa nie zalecamy zmniejszania tej liczby. Jeśli użytkownik wprowadzi nieprawidłowe hasło określoną liczbę razy, konto użytkownika zostanie zablokowane na jedną godzinę. Możesz odblokować konto użytkownika tylko poprzez zmianę hasła.

   - Jeśli to konieczne, przesuń przełącznik na **Wyłączone**, aby zabronić użytkownikowi możliwość łączenia z aplikacją. Możesz wyłączyć konto, na przykład, gdy pracownik opuści teren firmy.
4. Na zakładce **Bezpieczeństwo uwierzytelniania** możesz określić ustawienia zabezpieczeń dla tego konta.
5. Na zakładce **Grupy** możesz dodać użytkownika do grup zabezpieczeń.
6. Na zakładce **Urządzenia** możesz przypisać urządzenia do użytkownika.

7. Na zakładce **Role** możesz przypisać role do użytkownika.
8. Kliknij **Zapisz**, aby zachować zmiany.

Zaktualizowane konto użytkownika pojawi się na liście użytkowników i grup bezpieczeństwa.

Edytowanie grupy użytkownika

Możesz edytować grupy wewnętrzne.

W celu edytowania grupy użytkowników:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Kliknij nazwę grupy użytkowników, którą chcesz edytować.
3. W otwartym oknie ustawień grupy zmień ustawienia grupy użytkowników:
   - **Nazwa**
   - **Opis**
4. Kliknij **Zapisz**, aby zachować zmiany.

Zaktualizowana grupa użytkowników pojawi się na liście użytkowników i grup użytkowników.

Dodawanie kont użytkowników do grupy wewnętrznej

Do grupy wewnętrznej możesz dodać tylko konta użytkowników wewnętrznych.

W celu dodania kont użytkowników do grupy wewnętrznej:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Zaznacz pola obok kont użytkowników, które chcesz dodać do grupy.
3. Kliknij przycisk **Przypisz grupę**.
4. W oknie **Przypisz grupę**, które zostanie otwarte, wybierz grupę, do której chcesz dodać konta użytkowników.
5. Kliknij przycisk **Przypisz**.

Konta użytkowników zostaną dodane do grupy.

Wskazywanie użytkownika jako właściciela urządzenia

Aby uzyskać informacje na temat przypisywania użytkownika jako właściciela urządzenia mobilnego, zobacz pomoc dla Kaspersky Security for Mobile.

W celu wskazania użytkownika jako właściciela urządzenia:

1. Jeżeli chcesz przypisać właściciela urządzenia podłączonego do wirtualnego Serwera administracyjnego, najpierw przełącz się na wirtualny Serwer administracyjny:
   a. W menu głównym kliknij ikonę jodełki (›) po prawej stronie bieżącej nazwy Serwera administracyjnego.
   b. Wybierz wymagany Serwer administracyjny.
2. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
   Zostanie otwarta lista użytkowników. Jeśli jesteś aktualnie połączony z wirtualnym Serwerem administracyjnym, lista zawiera użytkowników z bieżącego wirtualnego Serwera administracyjnego oraz podstawowego Serwera administracyjnego.
3. Kliknij nazwę konta użytkownika, które chcesz przypisać jako właściciel urządzenia.
4. W otwartym oknie ustawień użytkownika kliknij zakładkę **Urządzenia**.
5. Kliknij **Dodaj**.
6. Z listy urządzeń wybierz urządzenie, które chcesz przypisać do użytkownika.
7. Kliknij **OK**.

Wybrane urządzenie zostanie dodane do listy urządzeń przypisanych do użytkownika.

To samo działanie możesz wykonać w **Urządzenia** → **Zarządzane urządzenia**, klikając nazwę urządzenia, które chcesz przypisać, a następnie klikając odnośnik **Zarządzaj właścicielem urządzenia**.

Usuwanie użytkownika lub grupy bezpieczeństwa

Możesz usunąć tylko użytkowników wewnętrznych lub wewnętrzne grupy bezpieczeństwa.

W celu usunięcia użytkownika lub grupy bezpieczeństwa:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Zaznacz pole obok użytkownika lub grupy bezpieczeństwa, którą chcesz usunąć.
3. Kliknij **Usuń**.
4. W otwartym oknie potwierdzenia kliknij **OK**.

Użytkownik lub grupa bezpieczeństwa zostanie usunięta.

Tworzenie roli użytkownika

W celu utworzenia roli użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij **Dodaj**.
3. W oknie **Nazwa nowej roli**, które zostanie otwarte, wprowadź nazwę nowej roli.
4. Kliknij **OK**, aby zastosować zmiany.
5. W oknie właściwości roli, które zostanie otwarte, zmień ustawienia roli:
   - Na zakładce **Ogólne** edytuj nazwę roli.
     Nie możesz edytować nazwy predefiniowanej roli.
   - Na zakładce **Ustawienia** edytuj obszar roli oraz zasady i profile skojarzone z rolą.
   - Na zakładce **Prawa dostępu** edytuj uprawnienia dostępu do aplikacji firmy Kaspersky.
6. Kliknij **Zapisz**, aby zachować zmiany.

Nowa rola pojawi się na liście ról użytkownika.

Edytowanie roli użytkownika

W celu edytowania roli użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij nazwę roli, którą chcesz edytować.
3. W oknie właściwości roli, które zostanie otwarte, zmień ustawienia roli:
   - Na zakładce **Ogólne** edytuj nazwę roli.
     Nie możesz edytować nazwy predefiniowanej roli.
   - Na zakładce **Ustawienia** edytuj obszar roli oraz zasady i profile skojarzone z rolą.
   - Na zakładce **Prawa dostępu** edytuj uprawnienia dostępu do aplikacji firmy Kaspersky.
4. Kliknij **Zapisz**, aby zachować zmiany.

Zaktualizowana rola pojawi się na liście ról użytkownika.

Edytowanie obszaru roli użytkownika

Obszar roli użytkownika to połączenie użytkowników i grup administracyjnych. Ustawienia skojarzone z rolą użytkownika są stosowane tylko do urządzeń, które należą do użytkowników posiadających tę rolę i tylko wtedy, gdy te urządzenia należą do grup skojarzonych z tą rolą, w tym grup potomnych.

W celu dodania użytkowników, grup bezpieczeństwa i grup administracyjnych do obszaru roli użytkownika, możesz użyć jednej z następujących metod:

Metoda 1:

1. W menu głównym przejdź do **Użytkownicy i role** → **Użytkownicy**.
2. Zaznacz pola obok użytkowników i grup bezpieczeństwa, które chcesz dodać do obszaru roli użytkownika.
3. Kliknij przycisk **Przypisz rolę**.

   Zostanie uruchomiony Kreator przypisywania roli. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
4. W kroku **Wybierz rolę** wybierz rolę użytkownika, którą chcesz przypisać.
5. W kroku **Zdefiniuj zakres** wybierz grupę administracyjną, którą chcesz dodać do obszaru roli użytkownika.
6. W celu zakończenia działania Kreatora kliknij przycisk **Przypisz rolę**.

Wybrani użytkownicy lub grupy bezpieczeństwa i wybrana grupa administracyjna zostaną dodane do obszaru roli użytkownika.

Metoda 2:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij nazwę roli, dla której chcesz określić obszar.
3. W otwartym oknie właściwości roli wybierz zakładkę **Ustawienia**.
4. W sekcji **Zakres roli** kliknij **Dodaj**.

   Zostanie uruchomiony Kreator przypisywania roli. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
5. W kroku **Zdefiniuj zakres** wybierz grupę administracyjną, którą chcesz dodać do obszaru roli użytkownika.
6. W kroku **Wybierz użytkowników** wybierz użytkowników i grupy zabezpieczeń, które chcesz dodać do obszaru roli użytkownika.
7. W celu zakończenia działania Kreatora kliknij przycisk **Przypisz rolę**.
8. Zamknij okno właściwości roli.

Wybrani użytkownicy lub grupy bezpieczeństwa i wybrana grupa administracyjna zostaną dodane do obszaru roli użytkownika.

Usuwanie roli użytkownika

W celu usunięcia roli użytkownika:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Zaznacz pole obok nazwy roli, którą chcesz usunąć.
3. Kliknij **Usuń**.
4. W otwartym oknie potwierdzenia kliknij **OK**.

Rola użytkownika zostanie usunięta.

Kojarzenie profili zasad z rolami

Możesz skojarzyć role użytkownika z profilami zasad. W tym przypadku reguła aktywacji dla tego profilu zasad jest oparta na roli: profil zasad staje się aktywny dla użytkownika, który posiada określoną rolę.

Na przykład, zasada zabrania wszelkich programów do nawigacji GPS na wszystkich urządzeniach w grupie administracyjnej. Program do nawigacji GPS jest wymagany tylko na jednym urządzeniu w grupie administracyjnej Użytkownicy—na urządzeniu, które należy do użytkownika zatrudnionego w charakterze kuriera. W tym przypadku możesz przypisać rolę „Kurier" do jego właściciela, a następnie utworzyć profil zasad zezwalający na uruchamianie programu do nawigacji GPS tylko na urządzeniach, których właściciele posiadają rolę „Kurier". Wszystkie pozostałe ustawienia zasady zostają zachowane. Tylko użytkownik z rolą „Kurier" będzie mógł uruchamiać program do nawigacji GPS. Później, jeśli innemu pracownikowi przypisano rolę „Kurier", nowy pracownik także może uruchomić program do nawigacji na urządzeniu należącym do organizacji. Uruchamianie programu do nawigacji GPS wciąż będzie zabronione na innych urządzeniach w tej samej grupie administracyjnej.

W celu skojarzenia roli z profilem zasad:

1. W menu głównym przejdź do **Użytkownicy i role** → **Role**.
2. Kliknij nazwę roli, którą chcesz skojarzyć z profilem zasad.
   Okno właściwości roli zostanie otwarte na wybranej zakładce **Ogólne**.
3. Wybierz zakładkę **Ustawienia** i przewiń w dół do sekcji **Profile zasad**.
4. Kliknij **Edytuj**.
5. W celu skojarzenia roli z:
   - **Istniejącym profilem zasad**—kliknij ikonę strzałki (›) obok nazwy żądanej zasady, a następnie zaznacz pole obok profilu, z którym chcesz skojarzyć rolę.
   - **Nowy profil zasad**:
     a. Zaznacz pole obok zasady, dla której chcesz utworzyć profil.
     b. Kliknij **Nowy profil zasad**.

c. Określ nazwę dla nowego profilu i skonfiguruj ustawienia profilu.

d. Kliknij przycisk **Zapisz**.

e. Zaznacz pole obok nowego profilu.

6. Kliknij **Przypisz do roli**.

Profil zostanie skojarzony z rolą i pojawi się we właściwościach roli. Profil jest stosowany automatycznie do dowolnego urządzenia, którego właścicielowi przypisano rolę.

Zarządzanie obiektami w Kaspersky Security Center Web Console

Ta sekcja zawiera informacje dotyczące zarządzania rewizjami obiektów. Kaspersky Security Center umożliwia śledzenie modyfikacji obiektów. Za każdym razem, gdy zapisujesz zmiany wprowadzone w obiekcie, tworzona jest *rewizja*. Każda rewizja posiada numer.

Obiekty aplikacji, które obsługują zarządzanie rewizjami, obejmują:

- Serwery administracyjne
- Zasady
- Zadania
- Grupy administracyjne
- Konta użytkowników
- Pakiety instalacyjne

Na rewizjach obiektów możesz wykonać następujące działania:

- Porównać wybraną rewizję z bieżącą rewizją
- Porównać wybrane rewizje
- Porównać obiekt wybranej rewizji z innym obiektem tego samego typu
- Przejrzeć wybraną rewizję
- Wycofać zmiany wprowadzone w obiekcie do wybranej rewizji
- Zapisać rewizje jako plik .txt

W oknie właściwości dowolnego obiektu obsługującego zarządzanie rewizjami sekcja **Historia rewizji** wyświetla listę rewizji obiektów z następującymi szczegółami:

- Liczbę rewizji obiektu
- Datę i godzinę modyfikacji obiektu
- Nazwę użytkownika, który zmodyfikował obiekt

- Działanie wykonane na obiekcie
- Opis rewizji związanej ze zmianą wprowadzoną w ustawieniach obiektu

Domyślnie, pole opisu rewizji obiektu jest puste. Aby dodać opis do rewizji, wybierz żądaną rewizję i kliknij przycisk **Opis**. W oknie **Opis rewizji obiektu** wprowadź opis rewizji.

Dodawanie opisu rewizji

Kaspersky Security Center umożliwia śledzenie modyfikacji obiektów. Za każdym razem, gdy zapisujesz zmiany wprowadzone w obiekcie, tworzona jest rewizja. Każda rewizja posiada numer.

Możesz dodać opis dla rewizji, aby uprościć wyszukiwanie rewizji na liście.

W celu dodania opisu rewizji:

1. Przejdź do sekcji **Historia rewizji** obiektu.
2. Na liście rewizji obiektu wybierz rewizję, dla której chcesz dodać opis.
3. Kliknij przycisk **Edytuj opis**.
   Zostanie otwarte okno **Opis**.
4. W oknie **Opis** wprowadź tekst do opisu wersji.
   Domyślnie, pole opisu rewizji obiektu jest puste.
5. Kliknij przycisk **Zapisz**.

Opis jest dodawany do wersji obiektu.

Usuwanie obiektów

Ta sekcja zawiera informacje dotyczące usuwania obiektów i przeglądania informacji o obiektach po ich usunięciu.

Możesz usuwać obiekty, w tym:

- Zasady
- Zadania
- Pakiety instalacyjne
- Wirtualne Serwery administracyjne
- Użytkownicy
- Grupy bezpieczeństwa
- Grupy administracyjne

Jeśli usuniesz obiekt, informacje o nim pozostaną w bazie danych. Okres przechowywania informacji o usuniętych obiektach jest taki sam, jak okres przechowywania rewizji obiektu (zalecany okres wynosi 90 dni). Możesz zmienić okres przechowywania tylko wtedy, gdy posiadasz uprawnienie **Modyfikacja** w obszarze uprawnień **Usunięte obiekty**.

Kaspersky Security Network (KSN)

Ta sekcja opisuje sposób korzystania z infrastruktury usług online o nazwie Kaspersky Security Network (KSN). Sekcja zawiera szczegóły dotyczące KSN, a także instrukcje związane z włączaniem KSN, konfiguracją dostępu do KSN oraz wyświetlaniem statystyk korzystania z serwera proxy KSN.

Informacje o KSN

Kaspersky Security Network (KSN) jest to usługa sieciowa oferująca dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky po wykryciu zagrożeń, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. KSN umożliwia korzystanie z baz danych reputacji firmy Kaspersky, z których pobierane są informacje o aplikacjach zainstalowanych na zarządzanych urządzeniach.

Kaspersky Security Center obsługuje następujące rozwiązania infrastrukturalne KSN:

- *Globalna sieć KSN* to rozwiązanie umożliwiające wymianę informacji z Kaspersky Security Network. Uczestnicząc w KSN, wyrażasz zgodę na wysyłanie do Kaspersky w trybie automatycznym informacji dotyczących działania aplikacji firmy Kaspersky, zainstalowanych na urządzeniach klienckich, które są zarządzane przez Kaspersky Security Center. Informacje są wysyłane zgodnie z bieżącymi ustawieniami dostępu KSN. Analitycy firmy Kaspersky dodatkowo analizują otrzymane informacje i umieszczają je w reputacyjnych i statystycznych bazach danych Kaspersky Security Network. Kaspersky Security Center domyślnie korzysta z tego rozwiązania.

- *Private KSN* to rozwiązanie, które umożliwia użytkownikom urządzeń z zainstalowanymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów. Kaspersky Private Security Network (Private KSN) jest przeznaczony dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z jednego z następujących powodów:

  - Urządzenia użytkowników nie są podłączone do internetu.

  - Przekazywanie jakichkolwiek danych poza granice kraju lub poza korporacyjną sieć LAN jest zabronione przez prawo lub ograniczone przez korporacyjną politykę bezpieczeństwa.

  Możesz skonfigurować ustawienia dostępu do Kaspersky Private Security Network w sekcji **Ustawienia KSN Proxy** w oknie właściwości Serwera administracyjnego.

Aplikacja wyświetla pytanie o przyłączenie się do KSN podczas działania kreatora wstępnej konfiguracji. Można rozpocząć lub zakończyć korzystanie z KSN w dowolnym momencie, podczas korzystania z aplikacji.

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji lub uaktualniania Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz nadal korzystać z KSN zgodnie z poprzednią wersją Oświadczenia KSN, które zaakceptowałeś wcześniej.

Gdy KSN jest włączone, Kaspersky Security Center sprawdza, czy serwery KSN są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić utrzymanie poziomu bezpieczeństwa zarządzanych urządzeń.

Urządzenia klienckie zarządzane przez Serwer administracyjny wchodzą w interakcję z KSN poprzez serwer proxy KSN. Serwer proxy KSN posiada następujące cechy:

- Urządzenia klienckie mogą wysyłać żądania do KSN oraz przesyłać informacje do KSN nawet wtedy, gdy nie mają bezpośredniego dostępu do internetu.
- Serwer KSN proxy buforuje przetwarzane dane, ograniczając obciążenie połączenia wychodzącego i czas oczekiwania na informacje żądane przez urządzenie klienckie.

Możesz skonfigurować serwer proxy KSN w sekcji **Ustawienia KSN Proxy** w oknie właściwości Serwera administracyjnego.

Konfigurowanie dostępu do KSN

Możesz skonfigurować dostęp do Kaspersky Security Network (KSN) na Serwerze administracyjnym i na punkcie dystrybucji.

W celu skonfigurowania dostępu Serwera administracyjnego do KSN:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

   Dane są wysyłane z urządzeń klienckich do KSN zgodnie z profilem Kaspersky Endpoint Security, który jest aktywny na tych urządzeniach klienckich. Jeśli to pole jest odznaczone, żadne dane nie będą wysyłane do KSN z Serwera administracyjnego i urządzeń klienckich poprzez Kaspersky Security Center. Jednakże urządzenia klienckie mogą wysyłać dane bezpośrednio do KSN (z pominięciem Kaspersky Security Center) zgodnie z ich ustawieniami. Profil Kaspersky Endpoint Security, aktywny na urządzeniach klienckich, określa, które dane będą wysyłane bezpośrednio z tych urządzeń do KSN (z pominięciem Kaspersky Security Center).

4. Przełącz przycisk przełącznika na pozycję **Użyj Kaspersky Security Network Włączono**.

   Jeśli ta opcja jest włączona, urządzenia klienckie będą wysyłać wyniki instalacji łat do Kaspersky. Przed włączeniem tej opcji należy przeczytać i zaakceptować warunki Oświadczenia KSN.

   Jeśli używasz Prywatnej sieci KSN, ustaw przycisk przełącznika w pozycji **Oświadczenie Kaspersky Private Security Network Włączone** i kliknij przycisk **Określ plik z ustawieniami KSN**, aby pobrać ustawienia prywatnej sieci KSN (pliki z rozszerzeniami pkcs7 i pem). Po pobraniu ustawień, interfejs wyświetla kontakty i nazwę dostawcy, a także datę utworzenia pliku z ustawieniami prywatnej sieci KSN.

   > Jeśli włączyłeś prywatną sieć KSN, zwróć uwagę na punkty dystrybucji skonfigurowane do wysyłania żądań KSN bezpośrednio do Cloud KSN. Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej) będzie nadal wysyłał żądania KSN do Cloud KSN. Aby ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do prywatnej sieci KSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji. Możesz włączyć tę opcję we właściwościach punktu dystrybucji lub w zasadzie Agenta sieciowego.

   Po ustawieniu przycisku przełącznika w pozycji **Oświadczenie Kaspersky Private Security Network Włączone**, pojawi się komunikat ze szczegółami dotyczącymi Prywatnej sieci KSN.

Prywatna sieć KSN jest obsługiwana przez następujące aplikacje firmy Kaspersky:

- Kaspersky Security Center
- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

Jeśli włączysz Prywatną sieć KSN w Kaspersky Security Center, te aplikacje otrzymają informację o obsłudze Prywatnej sieci KSN. W oknie ustawień aplikacji, w podsekcji **Kaspersky Security Network** sekcji **Zaawansowana ochrona przed zagrożeniami** wyświetlana jest informacja **Dostawca KSN: prywatna sieć KSN**. W innym przypadku, wyświetlana będzie informacja **Dostawca KSN: globalna sieć KSN**.

Jeśli podczas działania prywatnej sieci KSN korzystasz z wcześniejszej wersji aplikacji Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 lub Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent, zalecamy korzystanie z podrzędnych Serwerów administracyjnych, dla których włączono korzystanie z prywatnej sieci KSN.

Kaspersky Security Center nie wysyła żadnych danych statystycznych do Kaspersky Security Network, jeśli Prywatna sieć KSN została skonfigurowana w sekcji **Ustawienia KSN Proxy** okna właściwości Serwera administracyjnego.

5. Jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach Serwera administracyjnego, ale Twoja sieć wymaga, abyś korzystał bezpośrednio z prywatnej sieci KSN, włącz opcję **Ignoruj ustawienia serwera proxy w przypadku łączenia z Private KSN**. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do Private KSN.

6. Skonfiguruj połączenie Serwera administracyjnego z usługą KSN proxy:

   - W sekcji **Ustawienia połączenia**, w polu **Port TCP** określ numer portu TCP, który będzie używany do nawiązywania połączenia z serwerem proxy KSN. Domyślny port do nawiązywania połączenia z serwerem KSN proxy to 13111.
   - Jeśli chcesz, żeby Serwer administracyjny nawiązywał połączenie z serwerem proxy KSN poprzez port UDP, włącz opcję **Użyj portu UDP** i w polu **Port UDP** określ numer portu. Domyślnie opcja ta jest wyłączona i używany jest port TCP. Jeśli ta opcja jest włączona, domyślny port UDP do nawiązywania połączenia z serwerem KSN proxy to 15111.

7. Przełącz przycisk przełącznika na pozycję **Połącz podrzędne Serwery administracyjne z KSN przez główny Serwer administracyjny Włączone**.

   Jeśli ta opcja jest włączona, podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera KSN proxy. Jeśli ta opcja jest wyłączona, podrzędne Serwery administracyjne same łączą się z KSN. W tym przypadku zarządzane urządzenia używają podrzędnych Serwerów administracyjnych jako serwerów KSN proxy.

   Podrzędne Serwery administracyjne używają głównego Serwera administracyjnego jako serwera proxy, jeśli w prawej części sekcji **Ustawienia KSN Proxy**, dostępnej we właściwościach podrzędnych Serwerów administracyjnych, przycisk przełącznika jest ustawiony w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

8. Kliknij przycisk **Zapisz**.

   Ustawienia dostępu do KSN zostaną zapisane.

Możesz także skonfigurować dostęp punktu dystrybucji do KSN, na przykład, jeśli chcesz zmniejszyć obciążenie na Serwerze administracyjnym. Punkt dystrybucji działający jako serwer KSN proxy wysyła żądania KSN z zarządzanych urządzeń bezpośrednio do Kaspersky, bez używania Serwera administracyjnego.

W celu skonfigurowania dostępu punktu dystrybucji do Kaspersky Security Network (KSN):

1. Upewnij się, że punkt dystrybucji został przypisany ręcznie.
2. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
3. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.
4. Kliknij nazwę punktu dystrybucji, aby otworzyć okno właściwości.
5. W oknie właściwości punktu dystrybucji, w sekcji **KSN Proxy** włącz opcję **Włącz KSN Proxy po stronie punktu dystrybucji**, a następnie włącz opcję **Dostęp do KSN Cloud/Private KSN bezpośrednio przez Internet**.
6. Kliknij **OK**.

   Punkt dystrybucji będzie działał jako serwer KSN proxy.

Włączanie i wyłączanie KSN

W celu włączenia KSN:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.
3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Włączono**.

   Serwer KSN proxy zostanie włączony.
4. Przełącz przycisk przełącznika na pozycję **Użyj Kaspersky Security Network Włączono**.

   Usługa KSN zostanie włączona.

   Jeśli przycisk przełącznika jest włączony, urządzenia klienckie będą wysyłać wyniki instalacji poprawek do Kaspersky. Przed włączeniem tego przycisku przełącznika należy przeczytać i zaakceptować warunki Oświadczenia KSN.
5. Kliknij przycisk **Zapisz**.

W celu wyłączenia KSN:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.
2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Ustaw przycisk przełącznika w pozycji **Włącz KSN Proxy na Serwerze administracyjnym Wyłączono**, aby wyłączyć usługę KSN proxy lub ustawić przycisk przełącznika w pozycji **Użyj Kaspersky Security Network Wyłączono**.

   Jeśli jeden z tych przycisków przełączników jest wyłączony, urządzenia klienckie nie będą wysyłać wyników instalacji poprawek do Kaspersky.

   Jeśli korzystasz z Prywatnej sieci KSN, ustaw przycisk przełącznika w pozycji **Użyj Kaspersky Private Security Network Wyłączono**.

   Usługa KSN zostanie wyłączona.

4. Kliknij przycisk **Zapisz**.

Przeglądanie zaakceptowanego Oświadczenia KSN

Po włączeniu Kaspersky Security Network (KSN) musisz przeczytać i zaakceptować Oświadczenie KSN. W każdej chwili możesz przejrzeć zaakceptowane Oświadczenie KSN.

W celu przejrzenia zaakceptowanego Oświadczenia KSN:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Kliknij odnośnik **Zobacz Oświadczenie Kaspersky Security Network**.

W otwartym oknie możesz przejrzeć treść zaakceptowanego Oświadczenia KSN.

Akceptowanie zaktualizowanego Oświadczenia KSN

Korzystasz z KSN zgodnie z Oświadczeniem KSN, które czytasz i akceptujesz, gdy włączasz KSN. Jeśli Oświadczenie KSN zostanie zaktualizowane, zostanie wyświetlone podczas aktualizacji lub uaktualniania Serwera administracyjnego. Możesz zaakceptować zaktualizowane Oświadczenie KSN lub odrzucić je. Jeśli odrzucisz Oświadczenie, będziesz kontynuować korzystanie z KSN zgodnie z wersją Oświadczenia KSN, którą zaakceptowałeś wcześniej.

Po aktualizacji lub uaktualnieniu Serwera administracyjnego zaktualizowane Oświadczenie KSN jest wyświetlane automatycznie. Jeśli odrzucisz zaktualizowane Oświadczenie KSN, nadal możesz je przejrzeć i zaakceptować później.

W celu wyświetlenia, a następnie zaakceptowania lub odrzucenia zaktualizowanego Oświadczenia KSN:

1. Kliknij odnośnik **Wyświetl powiadomienia** znajdujący się w prawym górnym rogu okna głównego aplikacji.

   Zostanie otwarte okno **Powiadomienia**.

2. Kliknij odnośnik **Wyświetl zaktualizowane Oświadczenie KSN**.

   Zostanie otwarte okno **Aktualizacja Oświadczenia Kaspersky Security Network**.

3. Przeczytaj Oświadczenie KSN, a następnie podejmij decyzję, klikając jeden z następujących przycisków:

   - **Akceptuję zaktualizowane Oświadczenie KSN**

- **Użyj KSN w ramach starego Oświadczenia**

W zależności od Twojego wyboru KSN działa zgodnie z warunkami aktualnego lub zaktualizowanego Oświadczenia KSN. Możesz wyświetlić tekst zaakceptowanego Oświadczenia KSN we właściwościach Serwera administracyjnego w dowolnym momencie.

Sprawdzanie, czy punkt dystrybucji działa jako serwer proxy KSN

Na zarządzanym urządzeniu przypisanym do pracy jako punkt dystrybucji możesz włączyć serwer proxy KSN. Zarządzane urządzenie działa jako serwer proxy KSN, gdy usługa ksnproxy jest uruchomiona na urządzeniu. Możesz lokalnie sprawdzić, włączyć lub wyłączyć tę usługę na urządzeniu.

Jako punkt dystrybucji można przypisać urządzenie z systemem Windows lub Linux. Metoda sprawdzania punktu dystrybucji zależy od systemu operacyjnego tego punktu dystrybucji.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Windows działa jako serwer proxy KSN:

1. Na urządzeniu punktu dystrybucji, w systemie Windows otwórz **Usługi** (**Wszystkie programy** → **Narzędzia administracyjne** → **Usługi**).

2. Na liście usług sprawdź, czy usługa ksnproxy jest uruchomiona.

   Jeśli usługa ksnproxy jest uruchomiona, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Jeśli chcesz, możesz wyłączyć usługę ksnproxy. W takim przypadku Agent sieciowy w punkcie dystrybucji przestaje uczestniczyć w Kaspersky Security Network. To działanie wymaga uprawnień administratora lokalnego.

Aby sprawdzić, czy punkt dystrybucji oparty na systemie Linux działa jako serwer proxy KSN:

1. Na urządzeniu punktu dystrybucji wyświetl listę uruchomionych procesów.

2. Na liście uruchomionych procesów sprawdź, czy proces `/opt/kaspersky/ksc64/sbin/ksnproxy` jest uruchomiony.

Jeśli proces `/opt/kaspersky/ksc64/sbin/ksnproxy` jest uruchomiony, Agent sieciowy na urządzeniu uczestniczy w Kaspersky Security Network i działa jako serwer proxy KSN dla zarządzanych urządzeń należących do obszaru punktu dystrybucji.

Aktualizowanie baz danych i aplikacji Kaspersky

Ta sekcja opisuje kroki, które musisz podjąć, aby regularnie aktualizować następujące elementy:

- Baz danych i modułów oprogramowania firmy Kaspersky

- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

Scenariusz: Regularne aktualizowanie baz danych i aplikacji Kaspersky

Ta sekcja oferuje scenariusz regularnego aktualizowania baz danych, modułów i aplikacji firmy Kaspersky. Po zakończeniu Konfigurowania scenariusza ochrony sieci, musisz zachować niezawodność systemu ochrony, aby upewnić się, że Serwery administracyjne i zarządzane urządzenia są chronione przed różnymi zagrożeniami, w tym wirusami, atakami sieciowymi i atakami phishingowymi.

Aktualność ochrony sieci jest zapewniana przez regularne aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky
- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

Po zakończeniu tego scenariusza, możesz być pewny, że:

- Twoja sieć jest chroniona przez najaktualniejsze oprogramowanie firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające.
- Antywirusowe bazy danych i inne bazy danych Kaspersky krytyczne dla bezpieczeństwa sieci są zawsze aktualne.

Wymagania wstępne

Zarządzane urządzenia muszą mieć połączenie z Serwerem administracyjnym. Jeśli nie mają połączenia, rozważ ręczne zaktualizowanie baz danych, modułów i aplikacji Kaspersky lub bezpośrednio z serwerów aktualizacji Kaspersky.

Serwer administracyjny musi mieć połączenie z Internetem.

Przed rozpoczęciem upewnij się, że:

1. Wdrożono aplikacje zabezpieczające Kaspersky na zarządzanych urządzeniach zgodnie ze scenariuszem wdrażania aplikacji Kaspersky poprzez Kaspersky Security Center Web Console.
2. Utworzyłeś i skonfigurowałeś wszystkie wymagane profile, profile zasad i zadania zgodnie ze scenariuszem konfigurowania ochrony sieci.
3. Przydzieliłeś odpowiednią liczbę punktów dystrybucji zgodnie z liczbą zarządzanych urządzeń i topologią sieci.

Aktualizowanie baz danych i aplikacji Kaspersky odbywa się w etapach:

1. **Wybranie schematu aktualizacji**

   Istnieje kilka schematów, których możesz użyć do zainstalowania aktualizacji dla komponentów Kaspersky Security Center i aplikacji zabezpieczających. Wybierz schemat lub kilka schematów, które najlepiej spełniają wymagania Twojej sieci.

2. **Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego**

   To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Jeśli nie uruchamiałeś kreatora, utwórz zadanie teraz.

   To zadanie jest wymagane do pobrania uaktualnień z serwerów aktualizacji Kaspersky do repozytorium Serwera administracyjnego, a także do zaktualizowania baz danych i modułów Kaspersky dla aplikacji Kaspersky Security Center. Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

Jeśli w Twojej sieci są przypisane punkty dystrybucji, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. W tym przypadku zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.

Dostępne instrukcje:

- Konsola administracyjna: Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego
- Kaspersky Security Center Web Console: Tworzenie zadania pobierania uaktualnień do repozytorium Serwera administracyjnego

3. **Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji (opcjonalne)**

   Domyślnie, uaktualnienia są pobierane do punktów dystrybucji z Serwera administracyjnego. Możesz skonfigurować Kaspersky Security Center do pobierania uaktualnień do punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky. Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.

   Jeśli do Twojej sieci są przypisane punkty dystrybucji i utworzone jest zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, punkty dystrybucji pobiorą uaktualnienia z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji
   - Kaspersky Security Center Web Console: Tworzenie zadania pobierania uaktualnień do repozytoriów punktów dystrybucji

4. **Konfigurowanie punktów dystrybucji**

   Jeśli w Twojej sieci są przypisane punkty dystrybucji, upewnij się, że opcja **Roześlij aktualizacje** jest włączona we właściwościach wszystkich wymaganych punktów dystrybucji. Jeśli ta opcja jest włączona dla punktu dystrybucji, urządzenia znajdujące się w obszarze punktu dystrybucji pobierają uaktualnienia z repozytorium Serwera administracyjnego.

   Jeśli chcesz, żeby zarządzane urządzenia pobierały uaktualnienia tylko z punktów dystrybucji, włącz opcję **Rozsyłaj pliki tylko poprzez punkty dystrybucji** w zasadzie Agenta sieciowego.

5. **Optymalizowanie procesu aktualizacji przy użyciu trybu offline pobierania uaktualnień lub plików diff (opcjonalne)**

   Możesz zoptymalizować proces aktualizacji przy użyciu trybu offline pobierania uaktualnień (włączone domyślnie) lub przy użyciu plików diff. Dla każdego segmentu sieci musisz wybrać, którą z tych dwóch funkcji włączyć, ponieważ nie mogą działać jednocześnie.

   Jeśli tryb offline pobierania uaktualnień jest włączony, Agent sieciowy pobierze wymagane uaktualnienia na zarządzane urządzenie po pobraniu uaktualnień do repozytorium Serwera administracyjnego, zanim aplikacja zabezpieczająca zażąda uaktualnień. Zwiększy to niezawodność procesu aktualizacji. Aby korzystać z tej funkcji, włącz opcję **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)** w zasadzie Agenta sieciowego.

   Jeśli nie używasz trybu offline pobierania uaktualnień, możesz zoptymalizować ruch sieciowy między Serwerem administracyjnym a zarządzanymi urządzeniami przy użyciu plików diff. Jeśli ta funkcja jest włączona, Serwer administracyjny lub punkt dystrybucji pobierze pliki diff zamiast całych plików baz danych lub modułów Kaspersky. Plik diff opisuje różnice między dwoma wersjami pliku bazy danych lub modułu programu. Dlatego też plik diff zajmuje mniej miejsca niż cały plik. Spowoduje to zmniejszenie ruchu sieciowego między Serwerem administracyjnym lub punktami dystrybucji a zarządzanymi urządzeniami. Aby użyć tej funkcji, włącz opcję **Pobierz pliki diff** we właściwościach zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i/lub zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

Dostępne instrukcje:

- Używanie plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky
- Konsola administracyjna: Włączanie i wyłączanie trybu offline pobierania uaktualnień
- Kaspersky Security Center Web Console: Włączanie i wyłączanie trybu offline pobierania uaktualnień

6. **Sprawdzanie pobranych uaktualnień (opcjonalne)**

Przed zainstalowaniem pobranych uaktualnień możesz zweryfikować uaktualnienia poprzez zadanie *Weryfikacja uaktualnień*. To zadanie kolejno uruchamia zadania aktualizacji i zadania skanowania w poszukiwaniu złośliwego oprogramowania urządzeń, skonfigurowane poprzez ustawienia dla określonego zbioru urządzeń testowych. Po uzyskaniu wyników zadania, Serwer administracyjny uruchamia lub blokuje propagację aktualizacji na pozostałe urządzenia.

Zadanie *Weryfikacja uaktualnień* jest wykonywane jako część zadania *Pobierz uaktualnienia do repozytorium serwera administracyjnego*. We właściwościach zadania *Pobierz uaktualnienia do repozytorium serwera administracyjnego* włącz opcję **Zweryfikuj uaktualnienia przed rozesłaniem** w konsoli administracyjnej lub opcję **Uruchom weryfikację aktualizacji** w Kaspersky Security Center Web Console.

Dostępne instrukcje:

- Konsola administracyjna: Weryfikowanie pobranych uaktualnień
- Kaspersky Security Center Web Console: Weryfikowanie pobranych uaktualnień

7. **Zatwierdzanie i odrzucanie aktualizacji oprogramowania**

Domyślnie pobrane uaktualnienia oprogramowania posiadają stan *Niezdefiniowane*. Możesz zmienić stan na *Zatwierdzone* lub *Odrzucone*. Zatwierdzone aktualizacje są zawsze instalowane. Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia. Niezdefiniowane aktualizacje mogą zostać zainstalowane tylko na Agencie sieciowym, a inne komponenty Kaspersky Security Center zgodnie z ustawieniami zasady Agenta sieciowego. Aktualizacje, dla których ustawiłeś stan *Odrzucone*, nie zostaną zainstalowane na urządzeniach. Jeśli odrzucona aktualizacja dla aplikacji zabezpieczającej została wcześniej zainstalowana, Kaspersky Security Center spróbuje odinstalować aktualizację ze wszystkich urządzeń. Aktualizacje dla komponentów Kaspersky Security Center nie mogą zostać odinstalowane.

Dostępne instrukcje:

- Konsola administracyjna: Zatwierdzanie i odrzucanie aktualizacji oprogramowania
- Kaspersky Security Center Web Console: Zatwierdzanie i odrzucanie aktualizacji oprogramowania

8. **Konfigurowanie automatycznej instalacji uaktualnień i poprawek dla komponentów Kaspersky Security Center**

Pobrane aktualizacje i łaty dla Agenta sieciowego i innych komponentów Kaspersky Security Center są instalowane automatycznie. Jeśli pozostawiłeś opcję **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany** włączoną we właściwościach Agenta sieciowego, wówczas wszystkie uaktualnienia zostaną zainstalowane automatycznie po ich pobraniu do repozytorium (lub kilku repozytoriów). Jeśli ta opcja jest wyłączona, poprawki Kaspersky, które zostały pobrane i oznaczone jako *Niezdefiniowane*, zostaną zainstalowane dopiero po zmianie ich stanu na *Zatwierdzone*.

Dostępne instrukcje:

- Konsola administracyjna: Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center
- Kaspersky Security Center Web Console: Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center

9. **Instalacja uaktualnień dla Serwera administracyjnego**

   Aktualizacje oprogramowania dla Serwera administracyjnego nie zależą od stanów aktualizacji. Nie są instalowane automatycznie i muszą być wcześniej zatwierdzone przez administratora na zakładce **Monitorowanie** w Konsoli administracyjnej (**Serwer administracyjny** `<nazwa serwera>` → **Monitorowanie**) lub w sekcji **Powiadomienia** w Kaspersky Security Center Web Console (**Monitorowanie i raportowanie** → **Powiadomienia**). Następnie administrator musi wyraźnie uruchomić instalację uaktualnień.

10. **Konfigurowanie automatycznej instalacji uaktualnień dla aplikacji zabezpieczających**

    Utwórz zadania *Aktualizacji* dla zarządzanych aplikacji, aby zapewnić najnowsze aktualizacje aplikacji, modułów oprogramowania i baz danych Kaspersky, w tym antywirusowych baz danych. Aby zapewnić terminowe aktualizacje, zalecamy wybranie opcji **Po pobraniu nowych aktualizacji do repozytorium** podczas konfigurowania terminarza zadań.

    Jeśli Twoja sieć zawiera urządzenia obsługujące tylko protokół IPv6 i chcesz regularnie aktualizować aplikacje zabezpieczające zainstalowane na tych urządzeniach, upewnij się, że na zarządzanych urządzeniach zainstalowany jest Serwer administracyjny (w wersji nie wcześniejszej niż 13.2) oraz Agent sieciowy (w wersji nie wcześniejszej niż 13.2).

    Domyślnie, uaktualnienia dla Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Security for Linux są instalowane dopiero po zmianie stanu aktualizacji na *Zatwierdzone*. Ustawienia aktualizacji można zmienić w zadaniu *Aktualizacja*.

    Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia.

    Dostępne instrukcje:

    - Konsola administracyjna: Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach
    - Kaspersky Security Center Web Console: Automatyczna instalacja uaktualnień dla Kaspersky Endpoint Security na urządzeniach

Wyniki

Po zakończeniu scenariusza, Kaspersky Security Center jest konfigurowany do aktualizowania baz danych Kaspersky i zainstalowanych aplikacji Kaspersky po pobraniu uaktualnień do repozytorium Serwera administracyjnego lub do repozytoriów punktów dystrybucji. Możesz przejść do monitorowania stanu sieci.

Informacje o aktualizowaniu baz danych, modułów i aplikacji Kaspersky

W celu upewnienia się, że ochrona Serwerów administracyjnych i zarządzanych urządzeń jest aktualna, w odpowiednim czasie należy dostarczać aktualizacje:

- Baz danych i modułów oprogramowania firmy Kaspersky

  Przed pobraniem baz danych i modułów oprogramowania Kaspersky oprogramowanie Kaspersky Security Center sprawdza, czy serwery Kaspersky są dostępne. Jeżeli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja korzysta z publicznych serwerów DNS. Jest to konieczne, aby zapewnić aktualizację antywirusowych baz danych oraz zachować poziom bezpieczeństwa zarządzanych urządzeń.

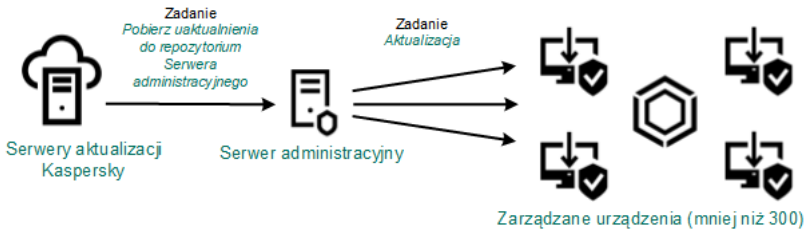
- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

W zależności od konfiguracji sieci, możesz użyć następujących schematów pobierania i rozsyłania żądanych aktualizacji na zarządzane urządzenia:

- Za pomocą jednego zadania: *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
- Używanie dwóch zadań:
  - Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*
  - Zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*
- Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP
- Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach
- Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Używanie zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego

W tym schemacie Kaspersky Security Center pobiera aktualizacje za pośrednictwem zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. W małych sieciach, które zawierają mniej niż 300 zarządzanych urządzeń w jednym segmencie sieci lub mniej niż 10 zarządzanych urządzeń w każdym segmencie sieci, aktualizacje są rozsyłane na zarządzane urządzenia bezpośrednio z repozytorium Serwera administracyjnego (patrz rysunek poniżej).

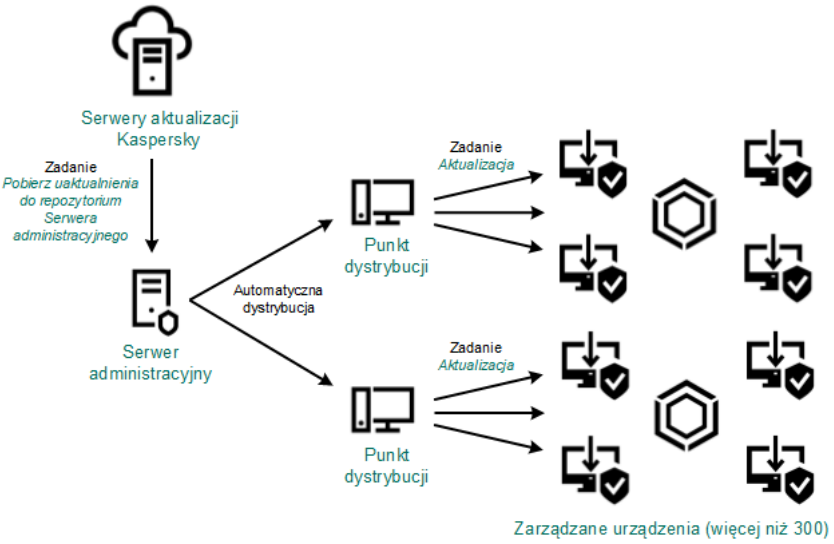


Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego bez punktów dystrybucji

Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

Jeśli sieć zawiera ponad 300 zarządzanych urządzeń w jednym segmencie sieci lub jeśli sieć zawiera kilka segmentów sieci z ponad 9 zarządzanymi urządzeniami w każdym segmencie sieci, zalecane jest użycie punktów dystrybucji do przesyłania aktualizacji na zarządzane urządzenia (patrz rysunek poniżej). Punkty dystrybucji zmniejszają obciążenie na Serwerze administracyjnym i optymalizują ruch sieciowy między Serwerem administracyjnym i zarządzanymi urządzeniami. Możesz obliczyć liczbę i konfigurację punktów dystrybucji wymaganych dla Twojej sieci.

W tym schemacie, uaktualnienia są automatycznie pobierane z repozytorium Serwera administracyjnego do repozytoriów punktów dystrybucji. Zarządzane urządzenia, znajdujące się w obszarze punktu dystrybucji, pobierają uaktualnienia z repozytorium punktu dystrybucji zamiast repozytorium Serwera administracyjnego.



Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego z punktami dystrybucji

Jeśli zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* zostało zakończone, z repozytorium Serwera administracyjnego zostają pobrane następujące aktualizacje:

- Bazy danych i moduły Kaspersky dla Kaspersky Security Center

  Te aktualizacje są instalowane automatycznie.

- Bazy danych i moduły Kaspersky dla aplikacji zabezpieczających na zarządzanych urządzeniach

  Te aktualizacje są instalowane poprzez zadanie Aktualizacja dla Kaspersky Endpoint Security for Windows.

- Aktualizacje dla Serwera administracyjnego

  Te aktualizacje nie są instalowane automatycznie. Administrator musi wyraźnie zatwierdzić i uruchomić instalację aktualizacji.

  > Uprawnienia lokalnego administratora są wymagane do zainstalowania łat na Serwerze administracyjnym.

- Aktualizacje dla komponentów Kaspersky Security Center

  Domyślnie, te aktualizacje są instalowane automatycznie. Możesz zmienić ustawienia w profilu Agenta sieciowego.

- Aktualizacje dla aplikacji zabezpieczających

  Domyślnie, Kaspersky Endpoint Security for Windows zainstaluje tylko te aktualizacje, które zatwierdzisz (aktualizacje możesz zatwierdzić za pośrednictwem Konsoli administracyjnej lub za pośrednictwem konsoli Kaspersky Security Center Web Console). Aktualizacje są instalowane poprzez zadanie *Aktualizacja* i mogą zostać skonfigurowane we właściwościach tego zadania.

> Zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego* nie jest dostępne na wirtualnych Serwerach administracyjnych. Repozytorium wirtualnego Serwera administracyjnego wyświetla uaktualnienia pobrane na główny Serwer administracyjny.

Możesz skonfigurować sprawdzanie aktualizacji pod kątem łatwości obsługi i błędów na zestawie urządzeń testowych. Jeśli weryfikacja zostanie zakończona pomyślnie, aktualizacje będą rozsyłane na inne zarządzane urządzenia.

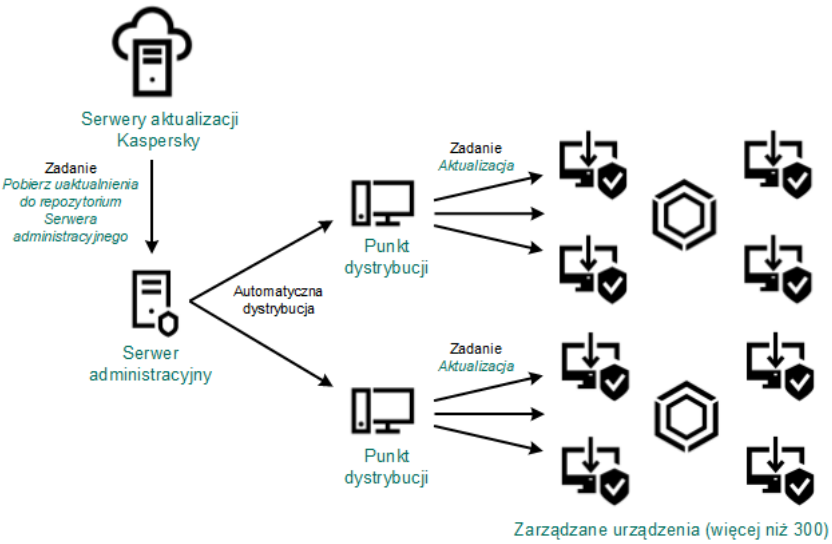
Każda aplikacja Kaspersky żąda wymaganych aktualizacji z Serwera administracyjnego. Serwer administracyjny gromadzi te żądania i pobiera tylko te uaktualnienia, które zostały zażądane przez aplikację. Dzięki temu te same uaktualnienia nie są pobierane kilka razy, a niepotrzebne uaktualnienia nie są pobierane wcale. Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, Serwer administracyjny automatycznie wysyła następujące informacje do serwerów aktualizacji Kaspersky w celu zapewnienia pobrania najnowszych wersji baz danych i modułów aplikacji Kaspersky:

- Identyfikator i wersja aplikacji
- Identyfikator instalacji aplikacji
- Identyfikator aktywnego klucza
- ID uruchamiania zadania *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*

Żadna z przesyłanych informacji nie zawiera danych osobowych ani innych poufnych danych. Firma AO Kaspersky Lab chroni informacje zgodnie z wymogami wynikającymi z przepisów prawa.

Używanie dwóch zadań: zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego oraz zadanie Pobierz aktualizacje do repozytoriów punktów dystrybucji

Możesz pobrać aktualizacje do repozytoriów punktów dystrybucji bezpośrednio z serwerów aktualizacji Kaspersky zamiast repozytorium Serwera administracyjnego, a następnie rozesłać aktualizacje na zarządzane urządzenia (patrz rysunek poniżej). Pobranie do repozytoriów punktów dystrybucji jest preferowane, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktami dystrybucji jest droższy niż ruch sieciowy pomiędzy punktami dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do internetu.



Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego oraz zadania Pobierz aktualizacje do repozytoriów punktów dystrybucji

Domyślnie, Serwer administracyjny i punkty dystrybucji komunikują się z serwerami aktualizacji Kaspersky i pobierają uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny i/lub punkty dystrybucji do używania protokołu HTTP zamiast HTTPS.

Aby zaimplementować ten schemat, utwórz zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* jako dodatek do zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Po pobraniu przez punkty dystrybucji aktualizacji z serwerów aktualizacji Kaspersky, a nie z repozytorium Serwera administracyjnego.

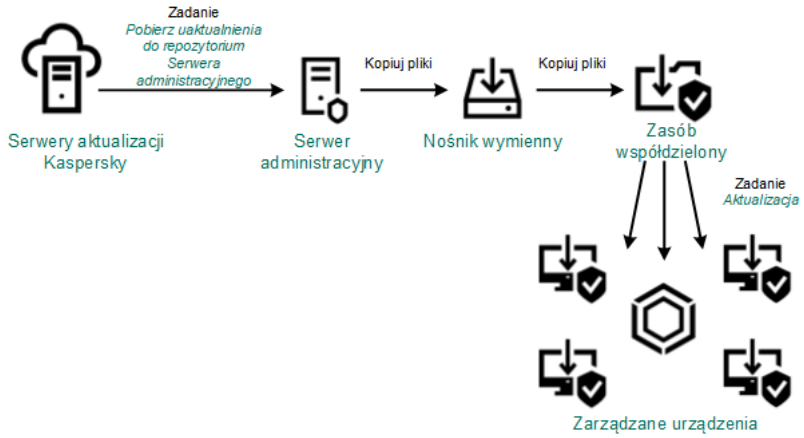
Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky.

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

Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* jest także wymagane dla tego schematu, ponieważ to zadanie jest używane do pobrania baz danych i modułów Kaspersky dla Kaspersky Security Center.

Ręcznie poprzez folder lokalny, folder współdzielony lub serwer FTP

Jeśli urządzenia klienckie nie mają połączenia z Serwerem administracyjnym, możesz użyć folderu lokalnego lub zasobu współdzielonego jako źródła dla aktualizacji baz danych, modułów i aplikacji Kaspersky. W tym schemacie możesz skopiować wymagane aktualizacje z repozytorium Serwera administracyjnego na dysk wymienny, a następnie skopiować aktualizacje do folderu lokalnego lub zasobu współdzielonego, określonego jako źródło uaktualnień w ustawieniach Kaspersky Endpoint Security (patrz rysunek poniżej).



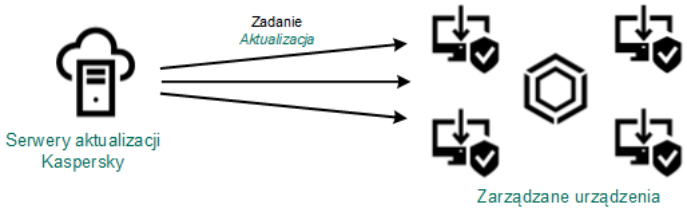
Aktualizowanie poprzez folder lokalny, folder współdzielony lub serwer FTP

Aby uzyskać więcej informacji na temat źródeł aktualizacji w Kaspersky Endpoint Security, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux — pomoc

Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security na zarządzanych urządzeniach

Na zarządzanych urządzeniach możesz skonfigurować Kaspersky Endpoint Security w celu pobierania aktualizacji bezpośrednio z serwerów aktualizacji Kaspersky (patrz rysunek poniżej).



W tym schemacie aplikacja zabezpieczająca nie używa repozytoriów dostarczonych przez Kaspersky Security Center. Aby pobierać uaktualnienia bezpośrednio z serwerów aktualizacji Kaspersky, określ serwery aktualizacji Kaspersky jako źródło uaktualnień w interfejsie aplikacji zabezpieczającej. Aby uzyskać więcej informacji na temat tych ustawień, zobacz następujące Pomoce:

- Pomoc Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux — pomoc

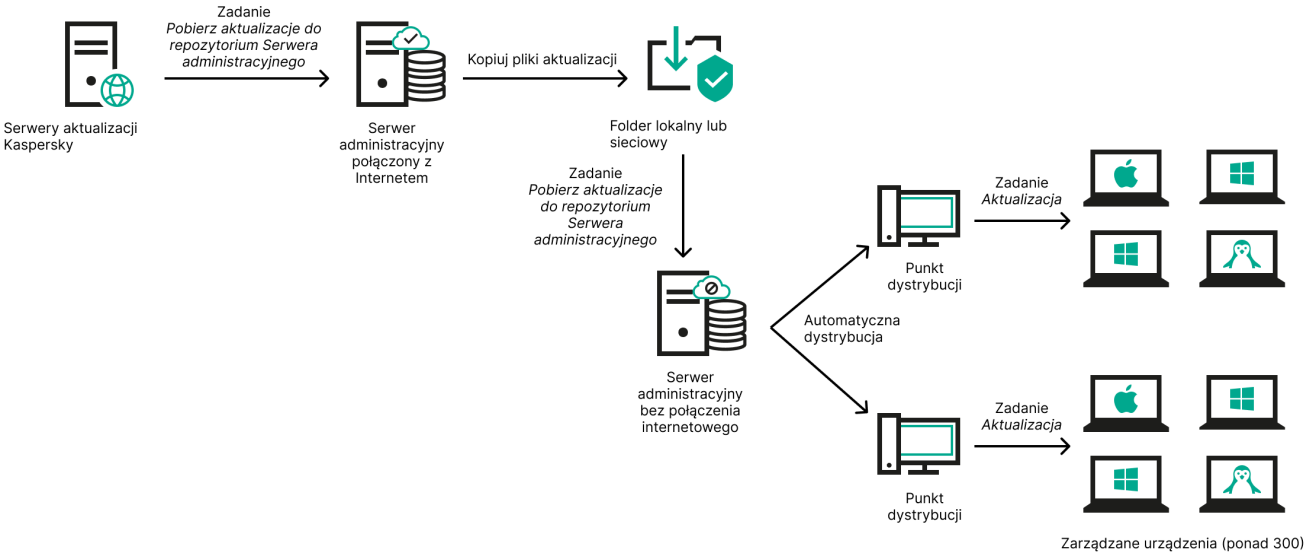
Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Jeżeli Serwer administracyjny nie ma połączenia z Internetem, możesz skonfigurować zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, aby pobierać uaktualnienia z folderu lokalnego lub sieciowego. W takim przypadku należy od czasu do czasu kopiować wymagane pliki aktualizacji do określonego folderu. Na przykład możesz skopiować wymagane pliki aktualizacji z jednego z następujących źródeł:

- Serwer administracyjny z połączeniem internetowym (patrz rysunek poniżej)

  Ponieważ serwer administracyjny pobiera tylko aktualizacje wymagane przez aplikacje zabezpieczające, zestawy aplikacji zabezpieczających zarządzanych przez serwery administracyjne — ten, który ma połączenie z Internetem i ten, który go nie ma — muszą być zgodne.

  Jeżeli Serwer administracyjny, którego używasz do pobierania uaktualnień, ma wersję 13.2 lub wcześniejszą, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.



Aktualizacja przez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

- Kaspersky Update Utility

  Ponieważ narzędzie to wykorzystuje stary schemat do pobierania uaktualnień, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.

Tworzenie zadania Pobierz aktualizacje do repozytorium serwera administracyjnego.

Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* Serwera administracyjnego jest automatycznie tworzone podczas działania Kreatora wstępnej konfiguracji Kaspersky Security Center. Możesz utworzyć tylko jedno zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Dlatego też zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* możesz utworzyć tylko wtedy, gdy takie zadanie zostało usunięte z listy zadań Serwera administracyjnego.

To zadanie jest wymagane do pobrania uaktualnień z serwera aktualizacji Kaspersky do repozytorium Serwera administracyjnego. Lista aktualizacji obejmuje:

- Aktualizacje baz danych i modułów dla Serwera administracyjnego
- Aktualizacje baz danych i modułów dla aplikacji zabezpieczających Kaspersky
- Aktualizacje komponentów Kaspersky Security Center
- Aktualizacje aplikacji zabezpieczających Kaspersky

Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

Przed dystrybucją aktualizacji do urządzeń zarządzanych możesz uruchomić zadanie *Weryfikacja uaktualnień*. Pozwala to upewnić się, że serwer administracyjny prawidłowo zainstaluje pobrane aktualizacje, a poziom bezpieczeństwa nie zmniejszy się z powodu aktualizacji. Aby zweryfikować je przed dystrybucją, skonfiguruj opcję **Uruchom weryfikację aktualizacji** w ustawieniach zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

*W celu utworzenia zadania **Pobierz aktualizacje do repozytorium Serwera administracyjnego**:*

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
6. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.
7. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.
8. W oknie właściwości zadania, na zakładce **Ustawienia aplikacji** określ następujące ustawienia:
   - Źródła aktualizacji

Jako źródła uaktualnień dla Serwera administracyjnego można użyć następujących zasobów:

- Serwery aktualizacji Kaspersky

  Serwery HTTP(S) firmy Kaspersky, z których aplikacje Kaspersky pobierają uaktualnienia baz danych i modułów aplikacji. Domyślnie, Serwer administracyjny komunikuje się z serwerami aktualizacji Kaspersky i pobiera uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny, aby używał protokołu HTTP zamiast HTTPS.

  Ta opcja jest wybrana domyślnie.

- Główny Serwer administracyjny

  Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

- Folder lokalny lub sieciowy

  Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

  Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

Jeśli folder współdzielony zawierający aktualizacje jest chroniony hasłem, włącz opcję **Określ konto, które posiada dostęp do udostępnionego folderu źródła aktualizacji (jeśli takie jest)** i wprowadź dane konta wymagane do uzyskania dostępu.

- Folder do przechowywania aktualizacji

  Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

- Inne ustawienia:

  - Wymuś aktualizację podrzędnych Serwerów administracyjnych

    Jeżeli ta opcja jest włączona, Serwer administracyjny uruchomi zadania aktualizacji na podrzędnych Serwerach administracyjnych zaraz po pobraniu nowych aktualizacji. W innym przypadku zadania aktualizacji na podrzędnych Serwerach administracyjnych będą uruchamiane zgodnie ze swoimi terminarzami.

    Domyślnie opcja ta jest wyłączona.

  - Kopiuj pobrane aktualizacje do dodatkowych folderów

Po otrzymaniu przez Serwer administracyjny uaktualnień skopiuje on je do określonych folderów. Użyj tej opcji, jeśli chcesz ręcznie zarządzać dystrybucją uaktualnień w sieci.

Na przykład, chcesz użyć tej opcji w następującej sytuacji: sieć Twojej organizacji zawiera kilka niezależnych podsieci, a urządzenia z każdej podsieci nie mają dostępu do innych podsieci. Jednakże urządzenia we wszystkich podsieciach mają dostęp do wspólnego udziału sieciowego. W tym przypadku skonfiguruj Serwer administracyjny w jednej z podsieci tak, aby pobierał uaktualnienia z serwerów aktualizacji Kaspersky, włącz tę opcję, a następnie określ ten udział sieciowy. W zadaniach pobierania uaktualnień do repozytorium dla innych Serwerów administracyjnych określ ten sam udział sieciowy jako źródło uaktualnień.

Domyślnie opcja ta jest wyłączona.

- **Nie wymuszaj aktualizacji urządzeń i podrzędnych Serwerów administracyjnych przed zakończeniem kopiowania**

  Zadania pobierania aktualizacji na urządzenia klienckie i podrzędne Serwery administracyjne zostaną uruchomione dopiero po skopiowaniu aktualizacji z głównego folderu aktualizacji do dodatkowych folderów aktualizacji.

  Ta opcja musi być włączona, jeśli urządzenia klienckie i podrzędne Serwery administracyjne pobierają aktualizacje z dodatkowych folderów sieciowych.

  Domyślnie opcja ta jest wyłączona.

- **Zawartość aktualizacji**:

  - **Pobierz pliki diff**

    Ta opcja włącza funkcję pobierania plików diff.

    Domyślnie opcja ta jest wyłączona.

- **Pobierz aktualizacje za pomocą starego schematu**

  Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

  Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

  - Kaspersky Update Utility

    To narzędzie pobiera aktualizacje przy użyciu starego schematu.

  - Kaspersky Security Center 13.2 lub wcześniejsza wersja

    Na przykład Twój serwer administracyjny 1 nie ma połączenia z Internetem. W takim przypadku możesz pobrać aktualizacje za pomocą serwera administracyjnego 2, który ma połączenie z Internetem, a następnie umieścić je w folderze lokalnym lub sieciowym, aby użyć go jako źródła uaktualnień dla serwera administracyjnego 1. Jeżeli serwer administracyjny 2 ma wersję 13.2 lub wcześniejszą, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu dla serwera administracyjnego 1.

  Domyślnie opcja ta jest wyłączona.

- **Uruchom weryfikację aktualizacji**

  Serwer administracyjny pobiera uaktualnienia ze źródła, zapisuje je w tymczasowym repozytorium i uruchamia zadanie określone w polu **Zadanie weryfikacji uaktualnień**. Jeśli zadanie zakończy się pomyślnie, uaktualnienia są kopiowane z tymczasowego repozytorium do folderu współdzielonego na Serwerze administracyjnym, a następnie są rozsyłane do wszystkich urządzeń, dla których Serwer administracyjny pełni rolę źródła uaktualnień (zadania są uruchamiane zgodnie z opcją terminarza - **Po pobraniu nowych uaktualnień do repozytorium**). Zadanie pobierania uaktualnień do repozytorium zostaje zakończone dopiero po zakończeniu zadania *weryfikacji uaktualnień*.

  Domyślnie opcja ta jest wyłączona.

9. W oknie właściwości zadania, na zakładce **Terminarz** utwórz terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

   - **Zaplanowane uruchomienie:**

     Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

     - **Ręcznie**

       Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

       Domyślnie opcja ta jest włączona.

     - **Co N minut**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

       Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

     - **Co N godzin**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

       Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

     - **Co N dni**

       Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

       Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

     - **Co N tygodni**

Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- **Co miesiąc, w określone dni wybranych tygodni**

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Po epidemii wirusa**

Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

- Ochrona antywirusowa stacji roboczych i serwerów plików
- Ochrona antywirusowa bram internetowych
- Ochrona antywirusowa serwerów pocztowych

Domyślnie, zaznaczone są wszystkie typy aplikacji.

Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest włączona.

- Używaj automatycznie losowego opóźnienia dla uruchamiania zadań

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)

Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

- **Zatrzymaj zadanie, jeżeli jest wykonywane dłużej niż (min)**

  Po minięciu określonego czasu, zadanie jest zatrzymywane automatycznie, niezależnie od tego, czy zostało zakończone.

  Włącz tę opcję, jeśli chcesz przerwać (lub zatrzymać) zadania, których wykonanie zajmuje zbyt dużo czasu.

  Domyślnie opcja ta jest wyłączona. Domyślny czas wykonania zadania to 120 minut.

10. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

Podczas wykonywania zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* uaktualnienia baz danych i modułów programu są pobierane ze źródła uaktualnień i przechowywane w folderze współdzielonym Serwera administracyjnego. Jeśli tworzysz to zadanie dla grupy administracyjnej, zostanie ono zastosowane tylko do Agentów sieciowych umieszczonych w określonej grupie administracyjnej.

Uaktualnienia są rozsyłane do urządzeń klienckich i podrzędnych Serwerów administracyjnych z folderu współdzielonego Serwera administracyjnego.

Sprawdzanie pobranych uaktualnień

Przed zainstalowaniem aktualizacji na zarządzanych urządzeniach, w pierwszej kolejności możesz sprawdzić aktualizacje pod kątem łatwości obsługi i błędów poprzez zadanie *Weryfikacja uaktualnień*. Zadanie *Weryfikacja uaktualnień* jest wykonywane automatycznie jako część zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Serwer administracyjny pobierze uaktualnienia ze źródła, zapisze je w repozytorium tymczasowym i uruchomi zadanie *weryfikacji uaktualnień*. Jeżeli zadanie zakończy się powodzeniem, uaktualnienia zostaną skopiowane z repozytorium tymczasowego do folderu współdzielonego na serwerze administracyjnym. Zostaną one rozesłane do wszystkich urządzeń klienckich, dla których Serwer administracyjny jest źródłem uaktualnień.

Jeżeli zadanie *weryfikacji uaktualnień* wykaże niepoprawność uaktualnień znajdujących się w repozytorium tymczasowym lub podczas wykonywania *tego zadania* wystąpi błąd, uaktualnienia nie zostaną skopiowane do folderu współdzielonego. Serwer administracyjny zachowa poprzedni zestaw uaktualnień. Zaplanowane zadania wykonywane zgodnie z opcją terminarza **Po pobraniu nowych aktualizacji do repozytorium** również nie zostaną uruchomione. Te działania są wykonywane podczas następnego uruchomienia zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, jeśli skanowanie nowych uaktualnień przebiegło bez problemów.

Zestaw uaktualnień jest uważany za nieprawidłowy, jeżeli przynajmniej na jednym urządzeniu testującym jest spełniony jeden z następujących warunków:

- Wystąpił błąd zadania aktualizacji.

- Stan ochrony w czasie rzeczywistym aplikacji zabezpieczającej zmienił się po zastosowaniu uaktualnień.
- W trakcie wykonywania zadania skanowania na żądanie wykryto zainfekowany obiekt.
- Wystąpił błąd w funkcjonowaniu programu firmy Kaspersky.

Jeśli żaden z powyższych warunków nie wystąpił na żadnym urządzeniu testującym, zestaw uaktualnień jest uważany za poprawny, a zadanie *weryfikacji uaktualnień* uważa się za zakończone pomyślnie.

Zanim zaczniesz tworzyć zadanie *Weryfikacja uaktualnień*, zrealizuj wymagania wstępne:

1. Utwórz grupę administracyjną z kilkoma urządzeniami testowymi. Ta grupa będzie potrzebna do weryfikacji uaktualnień.

   Zaleca się korzystanie z urządzeń z najbardziej niezawodną ochroną i najpowszechniejszą konfiguracją aplikacji w całej sieci. Takie podejście zwiększa jakość i prawdopodobieństwo wykrycia wirusa podczas skanowania oraz minimalizuje ryzyko fałszywych alarmów. Jeśli na urządzeniach testujących zostaną wykryte wirusy, zadanie *weryfikacji uaktualnień* zakończy się niepowodzeniem.

2. Utwórz zadania aktualizacji i skanowania w poszukiwaniu złośliwego oprogramowania do aplikacji obsługiwanej przez Kaspersky Security Center, na przykład Kaspersky Endpoint Security for Windows lub Kaspersky Security for Windows Server. Podczas tworzenia zadań aktualizacji i skanowania w poszukiwaniu złośliwego oprogramowania określ grupę administracyjną z urządzeniami testowymi.

   Zadanie *Weryfikacja uaktualnień* uruchamia kolejno zadania Aktualizacja i Skanowanie w poszukiwaniu złośliwego oprogramowania na urządzeniach testowych, aby sprawdzić, czy wszystkie aktualizacje są prawidłowe. Ponadto podczas tworzenia zadania *Weryfikacja uaktualnień* musisz określić zadania Aktualizacja i Skanowanie w poszukiwaniu złośliwego oprogramowania.

3. Utwórz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

W celu skonfigurowania Kaspersky Security Center do sprawdzania pobranych uaktualnień przed rozesłaniem ich na urządzenia klienckie:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij zadanie **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
3. W otwartym oknie właściwości zadania przejdź do zakładki **Ustawienia aplikacji**, a następnie włącz opcję **Uruchom weryfikację aktualizacji**.
4. Jeśli zadanie *weryfikacji aktualizacji* istnieje, kliknij przycisk **Wybierz zadanie**. W oknie, które zostanie otwarte, wybierz zadanie *Weryfikacja uaktualnień* w grupie administracyjnej z urządzeniami testowymi.
5. Jeśli wcześniej nie utworzono zadania *Weryfikacja uaktualnień*, wykonaj następujące czynności:

   a. Kliknij przycisk **Nowe zadanie**.

   b. W otwartym Kreatorze tworzenia nowego zadania określ nazwę zadania, jeśli chcesz zmienić wstępnie ustawioną nazwę.

   c. Wybierz grupę administracyjną z urządzeniami testowymi, którą utworzono wcześniej.

   d. Najpierw wybierz zadanie aktualizacji wymaganej aplikacji obsługiwanej przez Kaspersky Security Center, a następnie wybierz zadanie skanowania w poszukiwaniu złośliwego oprogramowania.

   Następnie pojawiają się następujące opcje. Zalecamy pozostawienie ich włączonych:

   - Uruchom urządzenie ponownie po aktualizacji baz danych

Po zaktualizowaniu antywirusowych baz danych na urządzeniu zalecamy ponowne uruchomienie urządzenia.

Domyślnie opcja ta jest włączona.

- **Sprawdź stan ochrony w czasie rzeczywistym po aktualizacji baz danych i ponownym uruchomieniu urządzenia**

  Jeżeli ta opcja jest włączona, zadanie *Weryfikacja uaktualnień* sprawdza, czy aktualizacje pobrane do repozytorium serwera administracyjnego są prawidłowe oraz czy poziom ochrony spadł po aktualizacji antywirusowej bazy danych i ponownym uruchomieniu urządzenia.

  Domyślnie opcja ta jest włączona.

e. Określ konto, z którego zostanie uruchomione zadanie *Weryfikacja uaktualnień*. Możesz użyć swojego konta i pozostawić włączoną opcję **Konto domyślne**. Alternatywnie można określić, że zadanie powinno być uruchamiane na innym koncie, które ma niezbędne prawa dostępu. Aby to zrobić, wybierz opcję **Określ konto**, a następnie wprowadź poświadczenia tego konta.

6. Kliknij **Zapisz**, aby zamknąć okno właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

Automatyczna weryfikacja uaktualnień zostanie włączona. Teraz możesz uruchomić zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, które rozpocznie się od weryfikacji aktualizacji.

Tworzenie zadania Pobierz uaktualnienia do repozytoriów punktów dystrybucji

Zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji* działa tylko na urządzeniach punktów dystrybucji działających pod kontrolą systemu operacyjnego Windows. Urządzenia punktów dystrybucji działające pod kontrolą systemu operacyjnego Linux lub macOS nie mogą pobierać uaktualnień z serwerów aktualizacji Kaspersky. Jeśli przynajmniej jedno urządzenie działające pod kontrolą systemu Linux lub macOS znajduje się w obszarze zadania, zadanie będzie posiadało stan *Niepowodzenie*. Nawet wtedy, gdy zadanie zakończyło się pomyślnie na wszystkich urządzeniach z systemem Windows, zwróci błąd na pozostałych urządzeniach.

Możesz utworzyć zadanie *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla grupy administracyjnej. To zadanie będzie uruchamiane dla punktów dystrybucji znajdujących się w określonej grupie administracyjnej.

Możesz użyć tego zadania, na przykład, jeśli ruch sieciowy pomiędzy Serwerem administracyjnym a punktem(ami) dystrybucji jest droższy niż ruch sieciowy pomiędzy punktem(ami) dystrybucji a serwerami aktualizacji Kaspersky lub jeśli Twój Serwer administracyjny nie ma dostępu do Internetu.

To zadanie jest wymagane do pobrania uaktualnień z serwerów aktualizacji Kaspersky do repozytoriów punktów dystrybucji. Lista aktualizacji obejmuje:

- Aktualizacje baz danych i modułów dla aplikacji zabezpieczających Kaspersky
- Aktualizacje komponentów Kaspersky Security Center
- Aktualizacje aplikacji zabezpieczających Kaspersky

Po pobraniu uaktualnień, mogą one zostać przesłane na zarządzane urządzenia.

*W celu utworzenia zadania **Pobierz aktualizacje do repozytoriów punktów dystrybucji** dla wybranej grupy administracyjnej:*

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center, w polu **Typ zadania** wybierz **Pobierz aktualizacje do repozytoriów punktów dystrybucji**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz przycisk opcji do określenia grupy administracyjnej, wyboru urządzeń lub urządzeń, do których stosowane jest zadanie.
6. W kroku **Zakończ tworzenie zadania**, jeśli chcesz zmienić domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
7. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.
8. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.
9. Na zakładce **Ustawienia aplikacji** okna właściwości zadania określ następujące ustawienia:

   - Źródła aktualizacji

     Jako źródła uaktualnień dla punktu dystrybucji można użyć następujących zasobów:

     - Serwery aktualizacji Kaspersky

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

       Opcja ta jest wybrana domyślnie.

     - Główny Serwer administracyjny

       Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.

     - Folder lokalny lub sieciowy

       Folder lokalny lub sieciowy, który zawiera najnowsze uaktualnienia. Folderem sieciowym może być serwer FTP lub HTTP lub udział SMB. Jeśli folder sieciowy wymaga uwierzytelnienia, obsługiwany jest tylko protokół SMB. Podczas wyboru folderu lokalnego powinieneś określić folder na urządzeniu z zainstalowanym Serwerem administracyjnym.

       Serwer FTP lub HTTP lub folder sieciowy używany przez źródło uaktualnień musi zawierać strukturę folderów (z uaktualnieniami), która odpowiada strukturze utworzonej podczas korzystania z serwerów aktualizacji Kaspersky.

- **Folder do przechowywania aktualizacji**

  Ścieżka do określonego folderu na potrzeby przechowywania zapisanych aktualizacji. Możesz skopiować ścieżkę do określonego folderu do schowka. Nie możesz zmienić ścieżki do określonego folderu w przypadku zadania grupowego.

- **Pobierz pliki diff**

  Ta opcja włącza funkcję pobierania plików diff.

  Domyślnie opcja ta jest wyłączona.

- **Pobierz aktualizacje za pomocą starego schematu**

  Począwszy od wersji 14, Kaspersky Security Center pobiera aktualizacje baz danych i modułów oprogramowania przy użyciu nowego schematu. Aby aplikacja pobierała aktualizacje przy użyciu nowego schematu, źródło aktualizacji musi zawierać pliki aktualizacji z metadanymi zgodnymi z nowym schematem. Jeśli źródło aktualizacji zawiera pliki aktualizacji z metadanymi zgodnymi tylko ze starym schematem, włącz opcję **Pobierz aktualizacje za pomocą starego schematu**. W przeciwnym razie zadanie pobierania aktualizacji zakończy się niepowodzeniem.

  Na przykład musisz włączyć tę opcję, gdy folder lokalny lub sieciowy jest określony jako źródło aktualizacji, a pliki aktualizacji w tym folderze zostały pobrane przez jedną z następujących aplikacji:

  - Kaspersky Update Utility

    To narzędzie pobiera aktualizacje przy użyciu starego schematu.

  - Kaspersky Security Center 13.2 lub wcześniejsza wersja

    Na przykład punkt dystrybucji jest skonfigurowany do pobierania aktualizacji z folderu lokalnego lub sieciowego. W takim przypadku aktualizacje można pobrać za pomocą serwera administracyjnego z połączeniem internetowym, a następnie umieścić je w folderze lokalnym w punkcie dystrybucji. Jeśli serwer administracyjny ma wersję 13.2 lub wcześniejszą, włącz opcję **Pobierz aktualizacje za pomocą starego schematu** w zadaniu *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

  Domyślnie opcja ta jest wyłączona.

10. Utwórz terminarz uruchamiania zadania. Jeśli to konieczne, określ następujące ustawienia:

- **Zaplanowane uruchomienie**

  Wybierz terminarz, zgodnie z którym uruchamiane jest zadanie, i skonfiguruj wybrany terminarz.

  - **Ręcznie**

    Zadanie nie jest uruchamiane automatycznie. Możesz je uruchomić tylko ręcznie.

    Domyślnie opcja ta jest włączona.

  - **Co N minut**

    Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonej godziny w dniu utworzenia zadania.

    Domyślnie, zadanie jest uruchamiane co 30 minut, począwszy od bieżącego czasu systemowego.

- **Co N godzin**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, zadanie jest uruchamiane co sześć godzin, począwszy od bieżącej daty i godziny systemowej.

- **Co N dni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Dodatkowo, możesz określić datę i godzinę pierwszego uruchomienia zadania. Te dodatkowe opcje staną się dostępne, jeśli są obsługiwane przez aplikację, dla której tworzysz zadanie.

  Domyślnie, zadanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N tygodni**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu, w określonym dniu tygodnia i o określonej godzinie.

  Domyślnie, zadanie jest uruchamiane w każdy poniedziałek o godzinie zgodnej z bieżącym czasem systemowym.

- **Codziennie (czas letni nie jest obsługiwany)**

  Zadanie jest uruchamiane regularnie, w określonych przedziałach czasu. Ten terminarz nie obsługuje czasu letniego (DST). Oznacza to, że gdy zegar przeskoczy o jedną godzinę do przodu lub tyłu na początku lub końcu DST, aktualny czas uruchomienia zadania nie ulegnie zmianie.

  Nie jest zalecane korzystanie z tego terminarza. Jest on potrzebny do wstecznej kompatybilności Kaspersky Security Center.

  Domyślnie, zadanie jest uruchamiane codziennie o godzinie zgodnej z bieżącym czasem systemowym.

- **Co tydzień**

  Zadanie jest uruchamiane co tydzień, w określonym dniu i o określonej godzinie.

- **Według dni tygodnia**

  Zadanie jest uruchamiane regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie zadanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc**

  Zadanie jest uruchamiane regularnie, w określonym dniu miesiąca i o określonej godzinie.

  W miesiącach, w które nie ma określonego dnia, zadanie jest uruchamiane w ostatnim dniu.

  Domyślnie, zadanie jest uruchamiane w pierwszym dniu każdego miesiąca, o godzinie zgodnej z bieżącym czasem systemowym.

- Co miesiąc, w określone dni wybranych tygodni

  Zadanie jest uruchamiane regularnie, w określone dni każdego miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- Po epidemii wirusa

  Zadanie jest uruchamiane po wystąpieniu zdarzenia *Epidemia wirusa*. Wybierz typy aplikacji, które będą monitorować epidemie wirusów. Dostępne są następujące typy aplikacji:

  - Ochrona antywirusowa stacji roboczych i serwerów plików
  - Ochrona antywirusowa bram internetowych
  - Ochrona antywirusowa serwerów pocztowych

  Domyślnie, zaznaczone są wszystkie typy aplikacji.

  Możesz chcieć uruchomić różne zadania w zależności od typu aplikacji antywirusowej, która zgłosiła epidemię wirusa. W tym przypadku, usuń wybór typów aplikacji, których nie potrzebujesz.

- Po zakończeniu wykonywania innego zadania

  Bieżące zadanie jest uruchamiane po zakończeniu innego zadania. Możesz wybrać sposób zakończenia poprzedniego zadania (pomyślnie lub z błędem), aby wyzwolić uruchomienie bieżącego zadania. Na przykład możesz chcieć uruchomić zadanie *Zarządzaj urządzeniami z opcją* **Włącz urządzenie** i, po zakończeniu jego wykonywania, uruchomić zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania*.

- Uruchom pominięte zadania

  Ta opcja określa zachowanie zadania, jeśli urządzenie klienckie nie jest widoczne w sieci, gdy zadanie ma zostać uruchomione.

  Jeżeli ta opcja jest włączona, system podejmie próbę uruchomienia zadania podczas kolejnego uruchomienia aplikacji Kaspersky na urządzeniu klienckim. Jeśli terminarz uruchamiania zadania jest ustawiony na **Ręcznie**, **Raz** lub **Natychmiast**, zadanie jest uruchamiane, gdy urządzenie stanie się widoczne w sieci lub od razu po uwzględnieniu urządzenia w obszarze zadania.

  Jeżeli ta opcja jest wyłączona, na urządzeniach klienckich będą uruchamiane tylko zaplanowane zadania, a dla trybu **Ręcznie**, **Raz** i **Natychmiast** zadania będą uruchamiane tylko na tych urządzeniach klienckich, które są widoczne w sieci. Na przykład, możesz chcieć wyłączyć tę opcję dla zadań zużywających duże ilości zasobów, które chcesz uruchamiać tylko poza godzinami pracy.

  Domyślnie opcja ta jest włączona.

- Używaj automatycznie losowego opóźnienia dla uruchamiania zadań

Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu, czyli z *rozproszonym uruchomieniem zadania*. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

Czas rozpoczęcia podjęcia próby uzyskania dostępu jest wyliczany automatycznie podczas tworzenia zadania, w zależności od liczby urządzeń klienckich, do których zadanie jest przypisane. Później zadanie będzie zawsze uruchamiane o wyliczonej godzinie uruchomienia. Jednakże, jeśli ustawienia zadania zostaną zmienione lub zadanie zostanie uruchomione ręcznie, zmieni się wyliczona wartość czasu uruchomienia zadania.

Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

- **Użyj losowego opóźnienia dla zadań uruchamianych w przedziale (min)**

  Jeśli ta opcja jest włączona, zadanie jest uruchamiane na urządzeniach klienckich losowo, w określonym przedziale czasu. Opcja ta pozwala uniknąć dużej liczby równoczesnych żądań wysyłanych przez urządzenia klienckie do Serwera administracyjnego, gdy uruchomione jest zaplanowane zadanie.

  Jeśli ta opcja jest wyłączona, zadanie jest uruchamiane na urządzeniach klienckich zgodnie z terminarzem.

  Domyślnie opcja ta jest wyłączona. Domyślny przedział czasu wynosi 1 minutę.

11. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

    Oprócz ustawień, które określasz podczas tworzenia zadania, możesz zmienić inne właściwości utworzonego zadania.

Po wykonaniu zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*, aktualizacje baz danych i modułów aplikacji zostaną pobrane ze źródła uaktualnień i będą przechowywane w folderze współdzielonym. Pobrane uaktualnienia zostaną użyte tylko przez punkty dystrybucji, które znajdują się w określonej grupie administracyjnej i dla których nie ustawiono zadania pobierania uaktualnień.

Włączanie i wyłączanie automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center

Aktualizacje i poprawki dla Serwera administracyjnego mogą zostać zainstalowane tylko ręcznie, po uzyskaniu wyraźnego zatwierdzenia przez administratora.

Automatyczna instalacja uaktualnień i łat dla komponentów Kaspersky Security Center jest włączona domyślnie podczas instalacji Agenta sieciowego na urządzeniu. Możesz to wyłączyć podczas instalacji Agenta sieciowego lub wyłączyć później przy użyciu profilu.

W celu wyłączenia automatycznej aktualizacji i instalacji poprawek dla komponentów Kaspersky Security Center podczas lokalnej instalacji Agenta sieciowego na urządzeniu:

1. Uruchom lokalną instalację Agenta sieciowego na urządzeniu.

2. W kroku **Ustawienia zaawansowane** odznacz pole **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**.

3. Postępuj zgodnie z instrukcjami kreatora.

   Na urządzeniu zostanie zainstalowany Agent sieciowy z wyłączoną automatyczną aktualizacją i instalacją łat dla komponentów Kaspersky Security Center. Automatyczne aktualizowanie i instalowanie poprawek można włączyć w późniejszym czasie, korzystając z profilu.

W celu wyłączenia automatycznego aktualizowania i instalowania poprawek dla komponentów Kaspersky Security Center podczas instalacji Agenta sieciowego na urządzeniu przy użyciu pakietu instalacyjnego:

1. W menu głównym przejdź do **Operacje** → **Repozytoria** → **Pakiety instalacyjne**.

2. Kliknij pakiet **Agent sieciowy Kaspersky Security Center <numer wersji>**.

3. W oknie właściwości otwórz zakładkę **Ustawienia**.

4. Wyłącz przycisk przełącznika **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**.

   Z tego pakietu zostanie zainstalowany Agent sieciowy z wyłączoną automatyczną aktualizacją i instalacją łat dla komponentów Kaspersky Security Center. Automatyczne aktualizowanie i instalowanie poprawek można włączyć w późniejszym czasie, korzystając z profilu.

Jeśli to pole zostało zaznaczone (lub odznaczone) podczas instalacji Agenta sieciowego na urządzeniu, możesz włączyć (lub wyłączyć) automatyczne aktualizowanie przy użyciu profilu Agenta sieciowa.

W celu włączenia lub wyłączenia automatycznego aktualizowania i instalowania poprawek dla składników Kaspersky Security Center przy użyciu profilu Agenta sieciowego:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.

2. Kliknij profil Agenta sieciowego.

3. W oknie ustawień zasady wybierz sekcję **Ustawienia aplikacji**.

4. W sekcji **Zarządzaj poprawkami i aktualizacjami** włącz lub wyłącz przycisk przełącznika **Automatycznie instaluj możliwe do zainstalowania aktualizacje i poprawki dla składników ze stanem Niezdefiniowany**, aby włączyć lub wyłączyć automatyczne aktualizowanie i instalowanie łat.

5. Ustaw blokadę (🔒) dla tego przycisku przełącznika.

   Profil zostanie zastosowany na wybranych urządzeniach, a automatyczne aktualizowanie i instalowanie poprawek dla komponentów Kaspersky Security Center zostanie włączone (lub wyłączone) na tych urządzeniach.

Pobieranie pakietu instalacyjnego dla Kaspersky Endpoint Security for Windows

Możesz skonfigurować automatyczne aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security for Windows na urządzeniach klienckich.

W celu skonfigurowania pobierania i automatycznej instalacji uaktualnień dla Kaspersky Endpoint Security for Windows na urządzeniach:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Endpoint Security for Windows, jako podtyp zadania wybierz **Aktualizacja**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz obszar zadania.
6. Określ grupę administracyjną, wybór urządzeń lub urządzenia, do których stosowane jest zadanie.
7. W kroku **Zakończ tworzenie zadania**, jeśli chcesz zmienić domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
8. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.
9. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.
10. Na zakładce **Ustawienia aplikacji** okna właściwości zadania zdefiniuj ustawienia zadania aktualizacji w trybie lokalnym lub mobilnym:

    - **Tryb lokalny**: Połączenie jest nawiązywane między urządzeniem a Serwerem administracyjnym.
    - **Tryb mobilny**: Połączenie pomiędzy Kaspersky Security Center a urządzeniem nie jest nawiązywane (na przykład, jeśli urządzenie nie jest podłączone do internetu).
11. Włącz źródło uaktualnień, którego chcesz użyć do zaktualizowania baz danych i modułów aplikacji dla Kaspersky Endpoint Security for Windows. Jeśli jest to wymagane, zmień pozycje źródeł na liście, korzystając z przycisków **W górę** i **W dół**. Jeśli włączonych jest kilka źródeł uaktualnień, Kaspersky Endpoint Security for Windows próbuje nawiązać z nimi połączenie po kolei, rozpoczynając od góry listy, i wykonać zadanie aktualizacji, pobierając pakiet aktualizacyjny z pierwszego dostępnego źródła.
12. Włącz opcję **Zainstaluj zatwierdzone aktualizacje modułów aplikacji**, aby pobrać i zainstalować uaktualnienia modułów aplikacji wraz z bazami danych aplikacji.

    Jeśli opcja jest włączona, Kaspersky Endpoint Security for Windows powiadamia użytkownika o dostępnych uaktualnieniach modułów aplikacji i włącza uaktualnienia modułów aplikacji do pakietu aktualizacyjnego podczas wykonywania zadania aktualizacji. Kaspersky Endpoint Security for Windows instaluje tylko te uaktualnienia, dla których ustawiłeś stan *Zatwierdzone*; zostaną zainstalowane lokalnie z poziomu interfejsu aplikacji lub poprzez Kaspersky Security Center.

    Możesz także włączyć opcję **Automatycznie instaluj krytyczne aktualizacje modułów aplikacji**. Jeśli dla modułów aplikacji dostępne są jakiekolwiek aktualizacje, Kaspersky Endpoint Security for Windows automatycznie zainstaluje te ze stanem *Krytyczne*. Pozostałe aktualizacje zostaną zainstalowane, jak je zatwierdzisz.

    Jeśli do zainstalowania uaktualnień modułów aplikacji wymagane jest przejrzenie i zaakceptowanie warunków Umowy licencyjnej i Polityki prywatności, aplikacja zainstaluje uaktualnienia po zaakceptowaniu warunków Umowy licencyjnej i Polityki prywatności przez użytkownika.

13. Zaznacz pole **Kopiuj uaktualnienia do folderu**, aby aplikacja zapisywała pobrane uaktualnienia w folderze, a następnie określ ścieżkę folderu.

14. Skonfiguruj terminarz zadania. Aby zapewnić dostarczanie aktualizacji na czas, zalecane jest włączenie opcji **Po pobraniu nowych uaktualnień do repozytorium**.

15. Kliknij **Zapisz**.

Podczas wykonywania zadania **Aktualizacja** aplikacja wysyła żądanie do serwerów aktualizacji Kaspersky.

Niektóre aktualizacje wymagają zainstalowania najnowszych wersji wtyczek zarządzających.

Zatwierdzanie i odrzucanie aktualizacji oprogramowania

Ustawienia zadania instalacji aktualizacji mogą wymagać zatwierdzenia aktualizacji, które mają zostać zainstalowane. Możesz zatwierdzić uaktualnienia, które muszą zostać zainstalowane, oraz odrzucić uaktualnienia, które nie muszą zostać zainstalowane.

Na przykład, możesz chcieć najpierw sprawdzić instalację aktualizacji w środowisku testowym i upewnić się, że nie wpływają negatywnie na działanie urządzeń, a następnie zezwolić na instalację tylko tych aktualizacji na urządzeniach klienckich.

W celu zatwierdzenia lub odrzucenia jednej lub kilku aktualizacji:

1. W menu głównym przejdź do **Operacje → Aplikacje Kaspersky → Aktualizacje oprogramowania Kaspersky**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

   Aktualizacje zarządzanych aplikacji mogą wymagać zainstalowania określonej minimalnej wersji Kaspersky Security Center. Jeśli ta wersja jest nowsza niż aktualna wersja, te aktualizacje są wyświetlane, ale nie można ich zatwierdzić. Ponadto żadne pakiety instalacyjne nie mogą być tworzone z takich aktualizacji, dopóki nie zaktualizujesz Kaspersky Security Center. Zostaniesz poproszony o uaktualnienie instancji Kaspersky Security Center do wymaganej wersji minimalnej.

2. Wybierz uaktualnienia, które chcesz zatwierdzić lub odrzucić.

3. Kliknij **Zatwierdź**, aby zatwierdzić wybrane aktualizacje, lub **Odrzuć**, aby odrzucić wybrane aktualizacje.

   Domyślna wartość to *Niezdefiniowane*.

Aktualizacje, do których przypisałeś stan *Zatwierdzono*, są umieszczane w kolejce do instalacji.

Aktualizacje, do których przypisałeś stan *Odrzucono*, są odinstalowywane (jeśli to możliwe) ze wszystkich urządzeń, na których były wcześniej zainstalowane. Dodatkowo, nie zostaną one zainstalowane na innych urządzeniach w przyszłości.

Niektórych uaktualnień dla aplikacji firmy Kaspersky nie można odinstalować. Jeśli ustawiłeś dla nich stan *Odrzucono*, Kaspersky Security Center nie odinstaluje tych uaktualnień z urządzeń, na których były wcześniej zainstalowane. Jednakże te uaktualnienia nigdy nie zostaną zainstalowane na innych urządzeniach w przyszłości.

Jeśli ustawisz stan *Odrzucono* dla aktualizacji oprogramowania firm trzecich, te aktualizacje nie zostaną zainstalowane na urządzeniach, dla których planowane było ich zainstalowanie, ale jeszcze nie zostały zainstalowane. Uaktualnienia pozostaną na urządzeniach, na których zostały już zainstalowane. Jeśli musisz usunąć aktualizacje, możesz je usunąć ręcznie lokalnie.

Aktualizowanie Serwera administracyjnego

Aktualizacje Serwera administracyjnego można zainstalować przy użyciu Uaktualnij moduły Serwera administracyjnego.

W celu zainstalowania aktualizacji Serwera administracyjnego:

1. W menu głównym przejdź do **Operacje** → **Aplikacje Kaspersky** → **Aktualizacje oprogramowania Kaspersky**.
2. Usuń Uaktualnij moduły Serwera administracyjnego w jeden z następujących sposobów:
   - Kliknij nazwę aktualizacji Serwera administracyjnego na liście aktualizacji, a następnie w oknie, które zostanie otwarte, kliknij odnośnik **Uruchom kreatora aktualizacji Serwera administracyjnego**.
   - Kliknij odnośnik **Uruchom kreatora aktualizacji Serwera administracyjnego** w polu powiadomień w górnej części okna.
3. W oknie Uaktualnij moduły Serwera administracyjnego wybierz jedną z poniższych opcji, aby określić, kiedy zainstalować aktualizację:
   - **Zainstaluj teraz**. Wybierz tę opcję, jeśli chcesz zainstalować aktualizację teraz.
   - **Odrocz instalację**. Wybierz tę opcję, jeśli chcesz zainstalować aktualizację później. W takim przypadku zostanie wyświetlone powiadomienie o tej aktualizacji.
   - **Ignoruj aktualizację**. Wybierz tę opcję, jeśli nie chcesz instalować aktualizacji i nie chcesz otrzymywać powiadomień o tej aktualizacji.
4. Wybierz opcję **Utwórz kopię zapasową Serwera administracyjnego przed rozpoczęciem instalacji aktualizacji**, jeśli chcesz utworzyć kopię zapasową Serwera administracyjnego przed zainstalowaniem aktualizacji.
5. W celu zakończenia działania Kreatora kliknij przycisk **OK**.

W przypadku przerwania procesu tworzenia kopii zapasowej przerywany jest również proces instalacji aktualizacji.

Włączanie i wyłączanie trybu offline pobierania uaktualnień

Nie jest zalecane wyłączanie trybu offline pobierania uaktualnień. Wyłączenie tego trybu może spowodować błędy w dostarczeniu uaktualnień na urządzenia. W niektórych przypadkach specjalista z pomocy technicznej Kaspersky może zalecić wyłączenie opcji **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem**. Następnie upewnij się, że zadanie pobierania uaktualnień dla aplikacji firmy Kaspersky zostało skonfigurowane.

W celu włączenia lub wyłączenia trybu offline pobierania uaktualnień dla grupy administracyjnej:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij **Grupy**.
3. W strukturze grupy administracyjnej należy wybrać grupę administracyjną, dla której chcesz włączyć tryb offline pobierania uaktualnień.
4. Kliknij profil Agenta sieciowego.

   Zostanie otwarte okno właściwości zasady Agenta sieciowego.

   Domyślnie, ustawienia profili potomnych są dziedziczone z profili nadrzędnych i nie mogą być modyfikowane. Jeśli profil, który chcesz zmodyfikować, jest dziedziczony, w pierwszej kolejności powinieneś utworzyć nowy profil dla Agenta sieciowego w żądanej grupie administracyjnej. W nowo utworzonym profilu możesz zmodyfikować ustawienia, które nie są zablokowane w profilu nadrzędnym.
5. Na zakładce **Ustawienia aplikacji** wybierz sekcję **Zarządzaj poprawkami i aktualizacjami**.
6. Włącz lub wyłącz opcję **Pobierz aktualizacje i antywirusowe bazy danych z Serwera administracyjnego z wyprzedzeniem (zalecane)**, aby włączyć lub wyłączyć model offline dla pobierania uaktualnień.

   Domyślnie włączony jest tryb offline pobierania uaktualnień.

Tryb offline pobierania uaktualnień zostanie włączony lub wyłączony.

Aktualizowanie baz danych i modułów Kaspersky na urządzeniach offline

Aktualizowanie baz danych i modułów Kaspersky na zarządzanych urządzeniach jest ważnym zadaniem do utrzymania ochrony urządzeń przed wirusami i innymi zagrożeniami. Administratorzy zazwyczaj konfigurują regularne aktualizacje poprzez używanie repozytorium Serwera administracyjnego lub repozytoriów punktów dystrybucji.

Jeśli musisz aktualizować bazy danych i moduły na urządzeniu (lub grupie urządzeń), które nie jest połączone z Serwerem administracyjnym (głównym lub podrzędnym), punktem dystrybucji lub internetem, musisz użyć alternatywnych źródeł uaktualnień, takich jak serwer FTP lub folder lokalny. W tym przypadku musisz dostarczyć pliki żądanych aktualizacji przy użyciu masowego urządzenia przechowywania, takiego jak dysk flash lub zewnętrzny dysk twardy.

Możesz skopiować wymagane aktualizacje z:

- Serwera administracyjnego.

  Aby mieć pewność, że repozytorium Serwera administracyjnego zawiera aktualizacje wymagane dla aplikacji zabezpieczającej zainstalowanej na urządzeniu offline, przynajmniej na jednym z zarządzanych urządzeń online musi być zainstalowana ta sama aplikacja zabezpieczająca. Ta aplikacja musi być skonfigurowana do pobierania aktualizacji z repozytorium Serwera administracyjnego poprzez zadanie Pobierz aktualizacje do repozytorium Serwera administracyjnego.

- Dowolne urządzenie, na którym ta sama aplikacja zabezpieczająca jest zainstalowana i skonfigurowana do pobierania uaktualnień z repozytorium Serwera administracyjnego, repozytorium punktu dystrybucji lub bezpośrednie z serwerów aktualizacji Kaspersky.

Poniżej znajduje się przykład konfigurowania aktualizacji baz danych i modułów poprzez kopiowanie ich z repozytorium Serwera administracyjnego.

W celu zaktualizowania baz danych i modułów Kaspersky na urządzeniach offline:

1. Podłącz dysk wymienny do urządzenia, na którym jest zainstalowany Serwer administracyjny.

2. Skopiuj pliki aktualizacji na dysk wymienny.

   Domyślnie, aktualizacje znajdują się w następującej lokalizacji: \\<nazwa serwera>\KLSHARE\Updates.

   Alternatywnie możesz skonfigurować Kaspersky Security Center do regularnego kopiowania uaktualnień do folderu, który wybierzesz. W tym celu użyj opcji **Kopiuj pobrane aktualizacje do dodatkowych folderów** we właściwościach zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego. Jeśli dla tej opcji określisz folder znajdujący się na dysku flash lub wewnętrznym dysku twardym jako folder docelowy, to urządzenie masowego przechowywania będzie zawsze zawierało najnowszą wersję aktualizacji.

3. Na urządzeniach offline skonfiguruj aplikację zabezpieczającą (na przykład, Kaspersky Endpoint Security for Windows), aby pobierała uaktualnienia z folderu lokalnego lub zasobu współdzielonego, takiego jak serwer FTP lub folder współdzielony.

4. Skopiuj pliki aktualizacji z dysku wymiennego do folderu lokalnego lub zasobu współdzielonego, którego chcesz użyć jako źródła uaktualnień.

5. Na urządzeniu offline, które wymaga zainstalowania aktualizacji, uruchom zadanie aktualizacji Kaspersky Endpoint Security for Windows.

Po zakończeniu zadania aktualizacji, bazy danych i moduły Kaspersky są aktualne na urządzeniu.

Tworzenie kopii zapasowych i przywracanie wtyczek webowych

Kaspersky Security Center Web Console umożliwia wykonanie kopii zapasowej bieżącego stanu wtyczki webowej, aby móc później przywrócić zapisany stan. Na przykład, możesz utworzyć kopię zapasową wtyczki webowej przed aktualizacją jej do nowszej wersji. Po aktualizacji, jeśli nowsza wersja nie spełnia Twoich wymagań lub oczekiwań, możesz przywrócić poprzednią wersję wtyczki webowej z kopii zapasowej.

W celu utworzenia kopii zapasowej wtyczek webowych:

1. W menu głównym przejdź do **Ustawienia konsoli** → **Wtyczki sieciowe**.

   Zostanie otwarte okno **Ustawienia konsoli**.

2. Na zakładce **Wtyczki sieciowe** wybierz wtyczki webowe, których kopię zapasową chcesz utworzyć, a następnie kliknij przycisk **Utwórz kopię zapasową**.

Kopia zapasowa wybranych wtyczek webowych zostanie utworzona. Utworzone kopie zapasowe można przeglądać na zakładce **Kopie zapasowe**.

W celu przywrócenia wtyczki webowej z kopii zapasowej:

1. W menu głównym przejdź do sekcji **Ustawienia konsoli** → **Kopie zapasowe**.

   Zostanie otwarte okno **Ustawienia konsoli**.

2. Na zakładce **Kopie zapasowe** wybierz kopię zapasową wtyczki webowej, którą chcesz przywrócić, a następnie kliknij przycisk **Przywróć z kopii zapasowej**.

Wtyczka webowa zostanie przywrócona z wybranej kopii zapasowej.

Dostosowanie punktów dystrybucji i bram połączenia

Struktura grup administracyjnych w Kaspersky Security Center pełni następujące funkcje:

- Tworzy zakres zasad

  Istnieje alternatywny sposób stosowania odpowiednich ustawień na urządzeniach przy użyciu *profili zasad*. W tym przypadku ustawiasz zakres zasad ze znacznikami, lokalizacjami urządzeń w jednostkach organizacyjnych Active Directory, członkostwem w grupach zabezpieczeń Active Directory.

- Tworzy zakres zadań grupowych

  Istnieje sposób określania zakresu zadań grupowych, który nie jest oparty na hierarchii grup administracyjnych: korzystanie z zadań dla wyboru urządzeń oraz z zadań dla wskazanych urządzeń.

- Nadaje urządzeniom, wirtualnym Serwerom administracyjnym oraz podrzędnym Serwerom administracyjnym prawa dostępu

- Przypisuje punkty dystrybucji

Podczas tworzenia struktury grup administracyjnych należy wziąć pod uwagę topologię sieci organizacji dla optymalnego przydzielenia punktów dystrybucji. Optymalne przydzielenie punktów dystrybucji pozwala na zmniejszenie ruchu w sieci organizacji.

W zależności od schematu organizacyjnego oraz topologii sieci, w strukturze grup administracyjnych można zastosować następujące standardowe konfiguracje:

- Jedno biuro

- Wiele małych, zdalnych biur

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

Standardowa konfiguracja punktów dystrybucji: Jedno biuro

W standardowej konfiguracji „jedno biuro" wszystkie urządzenia znajdują się w obrębie sieci organizacji i są dla siebie widoczne. Sieć organizacji może zawierać kilka oddzielnych części (sieci lub fragmentów sieci) połączonych ze sobą wąskimi kanałami.

Dostępne są następujące metody tworzenia struktury grup administracyjnych:

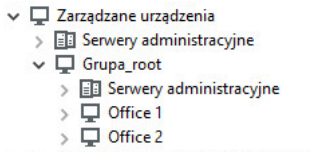
- Tworzenie struktury grup administracyjnych z uwzględnieniem topologii sieci. Struktura grup administracyjnych nie musi odzwierciedlać topologii sieci z absolutną dokładnością. Wystarczy dopasowanie oddzielnych części sieci i pewnych grup administracyjnych. Możesz skorzystać z automatycznego przydzielenia punktów dystrybucji lub zrobić to ręcznie.

- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie punktów dystrybucji, a następnie wskazać jedno lub kilka urządzeń jako punkty dystrybucji dla głównej grupy administracyjnej w każdej z oddzielnych części sieci, na przykład dla grupy **Zarządzane urządzenia**. Wszystkie punkty dystrybucji będą na tym samym poziomie i będą obejmować ten sam obszar, uwzględniając wszystkie urządzenia w sieci organizacji. W takim przypadku każdy z Agentów sieciowych połączy się z punktem dystrybucji o najkrótszej trasie. Trasę do punktu dystrybucji można ustalić za pomocą narzędzia tracert.

Standardowa konfiguracja punktów dystrybucji: Małe zdalne biura

Ta standardowa konfiguracja została utworzona z myślą o małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem internetu. Każde zdalne biuro znajduje się poza NAT, czyli połączenie jednego zdalnego biura z innym jest niemożliwe, gdyż biura są od siebie odizolowane.

Konfiguracja musi być odzwierciedlona w strukturze grup administracyjnych: dla każdego zdalnego biura musi zostać utworzona oddzielna grupa administracyjna (grupy **Office 1** i **Office 2** na rysunku poniżej).



Zdalne biura uwzględnione w strukturze grupy administracyjnej

Do każdej grupy administracyjnej odpowiadającej biuru należy przydzielić jeden lub kilka punktów dystrybucji. Punktami dystrybucji muszą być urządzenia w zdalnym biurze, które posiadają wystarczającą ilość wolnego miejsca na dysku. Urządzenia z grupy **Office 1** będą, na przykład, łączyć się z punktami dystrybucji przydzielonymi do grupy administracyjnej **Office 1**.

Jeśli niektórzy użytkownicy poruszają się między biurami ze swoimi laptopami, w każdym zdalnym biurze, dla grupy administracyjnej najwyższego poziomu (**Główna grupa dla biur** na poniższym rysunku) należy wskazać dwa lub więcej urządzeń jako punkty dystrybucji (oprócz już istniejących punktów dystrybucji).

Na przykład: Laptop znajduje się w grupie administracyjnej **Office 1**, a następnie zostaje fizycznie przeniesiony do biura, które odpowiada grupie administracyjnej **Office 2**. Po przeniesieniu laptopa, Agent sieciowy spróbuje połączyć się z punktami dystrybucji przypisanymi do grupy **Office 1**, ale te punkty dystrybucji są niedostępne. Następnie Agent sieciowy próbuje połączyć się z punktami dystrybucji, które zostały przypisane do **Głównej grupy dla biur**. Ponieważ zdalne biura są odizolowane od siebie, próby nawiązania połączenia z punktami dystrybucji przypisanymi do grupy administracyjnej **Główna grupa dla biur** zakończą się pomyślnie tylko wtedy, gdy Agent sieciowy spróbuje połączyć się z punktami dystrybucji w grupie **Office 2**. Oznacza to, że laptop pozostanie w grupie administracyjnej, która odpowiada pierwszemu biuru, ale będzie korzystał z punktu dystrybucji biura, w którym aktualnie się znajduje.

Informacje o przypisywaniu punktów dystrybucji

Możesz przypisać zarządzane urządzenie jako punkt dystrybucji ręcznie lub automatycznie.

Jeśli ręcznie przypiszesz zarządzane urządzenie jako punkt dystrybucji, możesz wybrać dowolne urządzenie w swojej sieci.

Jeśli przypiszesz punkty dystrybucji automatycznie, Kaspersky Security Center może wybrać tylko zarządzane urządzenie, które spełnia następujące warunki:

- Na urządzeniu jest przynajmniej 50 GB wolnej przestrzeni na dysku.
- Zarządzane urządzenie jest połączone bezpośrednio z Kaspersky Security Center (nie przez bramę).
- Zarządzane urządzenie nie jest laptopem.

> Jeśli w Twojej sieci nie ma urządzeń spełniających określone warunki, Kaspersky Security Center nie przypisze automatycznie żadnego urządzenia jako punktu dystrybucji.

Automatyczne przypisywanie punktów dystrybucji

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji.

Aby automatycznie przypisać punkty dystrybucji:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.
3. Wybierz opcję **Automatycznie przypisz punkty dystrybucji**.

   > Jeśli włączone jest automatyczne wskazywanie urządzeń jako punktów dystrybucji, nie można ręcznie skonfigurować punktów dystrybucji, ani też zmodyfikować listy punktów dystrybucji.

4. Kliknij przycisk **Zapisz**.

Serwer administracyjny automatycznie przypisze i skonfiguruje punkty dystrybucji.

Ręczne przypisywanie punktów dystrybucji

Kaspersky Security Center umożliwia ręczne wskazanie urządzeń do pełnienia roli punktów dystrybucji.

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center sam wybierze urządzenia, które mają być punktami dystrybucji. Jednakże, jeśli z jakiegoś powodu musisz zrezygnować z automatycznego przypisywania punktów dystrybucji (na przykład, jeśli chcesz korzystać ze specjalnie wybranych serwerów), możesz ręcznie przypisać punkty dystrybucji po obliczeniu ich liczby i konfiguracji.

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

W celu ręcznego wskazania urządzenia jako punktu dystrybucji:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

3. Wybierz opcję **Ręcznie przypisz punkty dystrybucji**.

4. Kliknij przycisk **Przypisz**.

5. Wybierz urządzenie, które ma być punktem dystrybucji.

   Podczas wybierania urządzenia pamiętaj o zasadach działania punktów dystrybucji i wymaganiach ustawionych dla urządzenia pełniącego rolę punktu dystrybucji.

6. Wybierz grupę administracyjną, którą chcesz uwzględnić w obszarze wybranego punktu dystrybucji.

7. Kliknij przycisk **OK**.

   Dodany punkt dystrybucji będzie wyświetlany na liście punktów dystrybucji, w sekcji **Punkty dystrybucji**.

8. Na liście kliknij nowo dodany punkt dystrybucji, aby otworzyć jego okno właściwości.

9. Skonfiguruj punkt dystrybucji w oknie właściwości:

   - Sekcja **Ogólne** zawiera ustawienie interakcji pomiędzy punktem dystrybucji a urządzeniami klienckimi:

     - **Port SSL**

       Numer portu SSL do nawiązywania zaszyfrowanych połączeń między urządzeniami klienckimi a punktem dystrybucji przy użyciu SSL.

       Domyślnie wykorzystywany jest port 13000.

     - **Użyj multiemisji**

       Jeśli ta opcja jest włączona, multicasting IP będzie używany do automatycznego rozsyłania pakietów instalacyjnych na urządzenia klienckie w obrębie grupy.

       Multiemisja IP zmniejsza czas wymagany do zainstalowania aplikacji z pakietu instalacyjnego w grupie urządzeń klienckich, ale zwiększa czas instalacji, gdy instalujesz aplikację na jednym urządzeniu klienckim.

     - **Adres multiemisji IP**

Adres IP, który będzie używany do multiemisji. Możesz zdefiniować adres IP z zakresu 224.0.0.0 – 239.255.255.255

Domyślnie, Kaspersky Security Center automatycznie przypisze unikatowy adres IP multiemisji w obrębie danego zakresu.

- **Numer portu multiemisji IP**

  Numer portu do multiemisji IP.

  Domyślnym numerem portu jest 15001. Jeśli jako punkt dystrybucji określono urządzenie, na którym działa Serwer administracyjny, domyślnie dla połączenia SSL używany jest port 13001.

- **Adres punktu dystrybucji dla urządzeń zdalnych**

  Adres IPv4, za pośrednictwem którego urządzenia zdalne łączą się z punktem dystrybucji.

- **Roześlij aktualizacje**

  Aktualizacje są dystrybuowane na zarządzane urządzenia z następujących źródeł:

  - Ten punkt dystrybucji, jeśli ta opcja jest włączona.
  - Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

  Jeśli używasz punktów dystrybucji do wdrażania aktualizacji, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

  Jeśli wyłączysz tę opcję, liczba pobrań aktualizacji i obciążenia Serwera administracyjnego mogą wzrosnąć. Domyślnie opcja ta jest włączona.

- **Roześlij pakiety instalacyjne**

  Pakiety instalacyjne są dystrybuowane na zarządzane urządzenia z następujących źródeł:

  - Ten punkt dystrybucji, jeśli ta opcja jest włączona.
  - Inne punkty dystrybucji, Serwer administracyjny lub serwery aktualizacji Kaspersky, jeśli ta opcja jest wyłączona.

  Jeśli używasz punktów dystrybucji do wdrażania pakietów instalacyjnych, możesz zmniejszyć ruch, ponieważ zmniejszasz liczbę pobrań. Możesz także odciążyć Serwer administracyjny i przenieść obciążenie między punktami dystrybucji. Możesz obliczyć liczbę punktów dystrybucji w Twojej sieci w celu optymalizacji ruchu i obciążenia.

  Jeśli wyłączysz tę opcję, liczba pobrań pakietów instalacyjnych i obciążenie Serwera administracyjnego może wzrosnąć. Domyślnie opcja ta jest włączona.

- **Uruchom serwer push**

W Kaspersky Security Center punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego oraz zarządzanych za pośrednictwem agenta sieciowego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

- **Port serwera push**

  Numer portu serwera push. Możesz określić numer dowolnego zajętego portu.

- W sekcji **Zakres** określ obszar, w jakim punkt dystrybucji będzie rozsyłał uaktualnienia (grupy administracyjne i/lub lokalizacja sieciowa).

  Tylko urządzenia działające pod kontrolą systemu operacyjnego Windows mogą determinować swoją lokalizację sieciową. Lokalizacja sieciowa nie może zostać określona dla urządzeń z zainstalowanymi innymi systemami operacyjnymi.

- Jeżeli punkt dystrybucji działa na komputerze innym niż Serwer administracyjny, w sekcji **Źródło aktualizacji** możesz wybrać źródło aktualizacji dla punktu dystrybucji:

  - **Źródło uaktualnień**

    Wybierz źródło uaktualnień dla punktu dystrybucji:

    - Aby zezwolić punktowi dystrybucji na pobieranie uaktualnień z Serwera administracyjnego, zaznacz opcję **Pobierz z Serwera administracyjnego**.
    - Aby umożliwić punktowi dystrybucji otrzymywanie aktualizacji za pomocą zadania, wybierz **Użyj zadania pobierania aktualizacji**, a następnie określ zadanie *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.
      - Jeśli takie zadanie już istnieje na urządzeniu, wybierz zadanie z listy.
      - Jeśli takie zadanie jeszcze nie istnieje na urządzeniu, kliknij łącze **Utwórz zadanie** , aby utworzyć zadanie. Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z instrukcjami kreatora.

  - **Pobierz pliki diff**

    Ta opcja włącza funkcję pobierania plików diff.

    Domyślnie opcja ta jest włączona.

- W podsekcji **Ustawienia połączenia z Internetem** możesz określić ustawienia dostępu do Internetu:

  - **Użyj serwera proxy**

Jeśli to pole jest zaznaczone, w polach wejściowych możesz skonfigurować połączenie z serwerem proxy.

Domyślnie pole to nie jest zaznaczone.

- **Adres serwera proxy**

  Adres serwera proxy.

- **Numer portu**

  Numer portu używanego do nawiązywania połączenia.

- **Pomiń serwer proxy dla adresów lokalnych**

  Jeśli ta opcja jest włączona, żaden serwer proxy nie będzie używany do nawiązywania połączenia z urządzeniami w sieci lokalnej.

  Domyślnie opcja ta jest wyłączona.

- **Uwierzytelnianie na serwerze proxy**

  Jeśli to pole jest włączone, w polach wejściowych możesz określić dane uwierzytelniające do autoryzacji na serwerze proxy.

  Domyślnie, pole to jest wyłączone.

- **Nazwa użytkownika**

  Konto użytkownika, z poziomu którego nawiązywane jest połączenie z serwerem proxy.

- **Hasło**

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

- W sekcji **KSN Proxy** możesz skonfigurować aplikację, aby używała punktu dystrybucji do przesyłania żądań KSN z zarządzanych urządzeń:

  - **Włącz KSN Proxy po stronie punktu dystrybucji**

Usługa KSN proxy jest uruchamiana na urządzeniu, które jest używane jako punkt dystrybucji. Użyj tej funkcji do redystrybucji i optymalizacji ruchu w sieci.

Punkt dystrybucji wysyła statystyki KSN, które zostały wymienione w Oświadczeniu Kaspersky Security Network, do Kaspersky. Domyślnie, Oświadczenie KSN znajduje się w %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Domyślnie opcja ta jest wyłączona. Włączenie tej opcji działa, jeśli opcje **Użyj Serwera administracyjnego jako serwera proxy** i **Zgadzam się na korzystanie z Kaspersky Security Network** zostały włączone w oknie właściwości Serwera administracyjnego.

Możesz przypisać węzeł klastra aktywny-pasywny do punktu dystrybucji i włączyć serwer proxy KSN na tym węźle.

- **Przesyłaj żądania KSN do Serwera administracyjnego**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do Serwera administracyjnego.

  Domyślnie opcja ta jest włączona.

- **Dostęp do KSN Cloud/Private KSN bezpośrednio przez Internet**

  Punkt dystrybucji przesyła żądania KSN z zarządzanych urządzeń do chmury KSN lub Private KSN. Żądania KSN wygenerowane na samym punkcie dystrybucji są także wysyłane bezpośrednio do chmury KSN lub Private KSN.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 11 (lub wcześniejszej), nie może uzyskać bezpośredniego dostępu do Private KSN. Jeśli chcesz ponownie skonfigurować punkty dystrybucji do wysyłania żądań KSN do prywatnej sieci KSN, włącz opcję **Przesyłaj żądania KSN do Serwera administracyjnego** dla każdego punktu dystrybucji.

  Punkty dystrybucji, na których jest zainstalowany Agent sieciowy w wersji 12 (lub późniejszej), może uzyskać bezpośredni dostęp do Private KSN.

- **Ignoruj ustawienia serwera proxy w przypadku łączenia z Private KSN**

  Włącz tę opcję, jeśli skonfigurowałeś ustawienia serwera proxy we właściwościach punktu dystrybucji lub w zasadzie Agenta sieciowego, ale architektura Twojej sieci wymaga bezpośredniego korzystania z Private KSN. W przeciwnym razie, żądania z zarządzanych aplikacji nie będą mogły dotrzeć do Private KSN.

  Ta opcja jest dostępna, jeśli wybierzesz opcję **Dostęp do KSN Cloud/Private KSN bezpośrednio przez Internet**.

- **Port**

  Numer portu TCP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny numer portu to 13111.

- **Użyj portu UDP**

  Jeśli chcesz, żeby zarządzane urządzenia nawiązywały połączenie z serwerem KSN proxy poprzez port UDP, włącz opcję **Użyj portu UDP** i określ numer portu UDP. Domyślnie opcja ta jest włączona.

- **Port UDP**

Numer portu UDP, którego zarządzane urządzenia będą używały do nawiązywania połączenia z serwerem KSN proxy. Domyślny port UDP do nawiązywania połączenia z serwerem KSN Proxy to 15111.

- Jeżeli punkt dystrybucji działa na komputerze innym niż Serwer administracyjny, w sekcji **Brama połączenia** możesz skonfigurować punkt dystrybucji tak, aby działał jako brama dla połączenia między instancjami Agenta sieciowego a Serwerem administracyjnym:

  - Brama połączenia

    Jeżeli bezpośrednie połączenie między Serwerem administracyjnym a Agentami sieciowymi nie może zostać nawiązane z powodu organizacji Twojej sieci, możesz użyć punktu dystrybucji, aby działał jako brama połączenia między Serwerem administracyjnym a Agentami sieciowymi.

    Włącz tę opcję, jeśli chcesz, aby punkt dystrybucji działał jako brama połączenia między Agentami sieciowymi a Serwerem administracyjnym. Domyślnie opcja ta jest wyłączona.

  - Nawiąż połączenie z bramą z poziomu Serwera administracyjnego (jeśli brama znajduje się w DMZ)

    Jeżeli Serwer administracyjny znajduje się poza strefą zdemilitaryzowaną (DMZ), w sieci lokalnej, Agenty sieciowe zainstalowane na zdalnych urządzeniach nie mogą łączyć się z Serwerem administracyjnym. Możesz użyć punktu dystrybucji jako bramy połączenia z odwrotną łącznością (Serwer administracyjny nawiązuje połączenie z punktem dystrybucji).

    Włącz tę opcję, jeśli chcesz połączyć Serwer administracyjny z bramą połączenia w strefie DMZ.

  - Otwórz port lokalny dla Kaspersky Security Center Web Console

    Włącz tę opcję, jeśli chcesz, aby brama połączenia w strefie DMZ otwierała port konsoli internetowej znajdujący się w strefie DMZ lub w Internecie. Określ numer portu, który będzie używany do połączenia z konsoli internetowej do punktu dystrybucji. Domyślny numer portu to 13299.

    Ta opcja jest dostępna, jeśli włączysz opcję **Nawiąż połączenie z bramą z poziomu Serwera administracyjnego (jeśli brama znajduje się w DMZ)**.

  - Otwórz port dla urządzeń mobilnych (tylko uwierzytelnianie SSL Serwera administracyjnego)

    Włącz tę opcję, jeśli potrzebujesz, aby brama połączenia otwierała port dla urządzeń mobilnych i określała numer portu, którego będą używać urządzenia mobilne do łączenia się z punktem dystrybucji. Domyślny numer portu to 13292. Podczas nawiązywania połączenia uwierzytelniany jest tylko Serwer administracyjny.

  - Otwórz port dla urządzeń mobilnych (wzajemne uwierzytelnianie SSL)

Włącz tę opcję, jeśli potrzebujesz bramy połączenia, aby otworzyć port, który będzie używany do dwukierunkowej autoryzacji Serwera administracyjnego i urządzeń mobilnych. Określ następujące parametry:

- Numer portu, którego urządzenia mobilne będą używać do łączenia się z punktem dystrybucji. Domyślny numer portu to 13293.
- Nazwy domen DNS bramy połączenia, które będą używane przez urządzenia mobilne. Oddziel nazwy domen przecinkami. Określone nazwy domen zostaną uwzględnione w certyfikacie punktu dystrybucji. Jeśli nazwy domen używane przez urządzenia mobilne nie są zgodne z nazwą wspólną w certyfikacie punktu dystrybucji, urządzenia mobilne nie łączą się z punktem dystrybucji.

  Domyślną nazwą domeny DNS jest nazwa FQDN bramy połączenia.

- Skonfiguruj przeszukiwanie domen Windows, Active Directory i zakresów IP przez punkt dystrybucji:
  - Domeny Windows

    Możesz włączyć wykrywanie urządzeń dla domen Windows i ustawić terminarz dla wyszukiwania.

  - Active Directory

    Możesz włączyć przeszukiwanie sieci dla Active Directory i ustawić terminarz dla przeszukiwania.

    Jeśli zaznaczysz pole **Enable Active Directory polling**, możesz wybrać jedną z następujących opcji:
    - **Przeszukaj bieżącą domenę Active Directory**.
    - **Przeszukaj las domen Active Directory**.
    - **Przeszukaj tylko wybrane domeny Active Directory**. Jeśli wybierzesz tę opcję, dodaj jedną lub kilka domen Active Directory do listy.

  - Zakresy IP

    Możesz włączyć wykrywanie urządzeń dla zakresów IPv4 i sieci IPv6.

    Jeśli włączysz opcję **Włącz przeszukiwanie zakresów**, możesz dodać skanowane zakresy i skonfigurować dla nich terminarz. Możesz dodać zakresy IP do listy skanowanych zakresów.

    Jeśli włączysz opcję **Użyj Zeroconf do przeszukiwania sieci IPv6**, punkt dystrybucji automatycznie odpytuje sieć IPv6 za pomocą zero-configuration networking (zwany również *Zeroconf*). W takim przypadku określone zakresy adresów IP są ignorowane, ponieważ punkt dystrybucji przeszukuje całą sieć. Opcja **Użyj Zeroconf do przeszukiwania sieci IPv6** jest dostępna, jeśli w punkcie dystrybucji działa system Linux. Aby korzystać z odpytywania Zerocong IPv6, musisz zainstalować narzędzie avahi-browse w punkcie dystrybucji.

- W sekcji **Zaawansowane** określ folder, którego punkt dystrybucji musi używać do przechowywania rozsyłanych danych:
  - Użyj folderu domyślnego

    Jeśli wybierzesz tę opcję, aplikacja użyje folderu instalacyjnego Agenta sieciowego na urządzeniu działającym jako punkt dystrybucji.

- Użyj określonego folderu

  Jeśli wybierzesz tę opcję, w polu poniżej możesz określić ścieżkę dostępu do wybranego folderu. Może to być folder lokalny na urządzeniu działającym jako punkt dystrybucji lub folder na dowolnym urządzeniu w obrębie sieci korporacyjnej.

  Konto użytkownika używane na urządzeniu działającym jako punkt dystrybucji do uruchamiania Agenta sieciowego musi mieć uprawnienia do odczytu/zapisu określonego folderu.

10. Kliknij przycisk **OK**.

    Wybrane urządzenia będą pełnić rolę punktów dystrybucji.

Modyfikowanie listy punktów dystrybucji dla grupy administracyjnej

Możesz wyświetlić listę punktów dystrybucji przypisanych do określonej grupy administracyjnej oraz zmodyfikować listę, dodając lub usuwając punkty dystrybucji.

W celu przejrzenia i zmodyfikowania listy punktów dystrybucji przypisanych do grupy administracyjnej:

1. W menu głównym przejdź do **Urządzenia** → **Grupy**.
2. W strukturze grupy administracyjnej należy wybrać grupę administracyjną, dla której chcesz przejrzeć przypisane punkty dystrybucji.
3. Wybierz zakładkę **Punkty dystrybucji**.
4. Dodaj nowe punkty dystrybucji dla grupy administracyjnej, korzystając z przycisku **Przypisz**, lub usuń przypisane punkty dystrybucji, korzystając z przycisku **Cofnij przypisanie**.

   W zależności od Twoich modyfikacji, nowe punkty dystrybucji są dodawane do listy lub istniejące punkty dystrybucji zostają usunięte z listy.

Wymuszona synchronizacja

Pomimo tego, że Kaspersky Security Center automatycznie synchronizuje stan, ustawienia, zadania i zasady dla zarządzanych urządzeń, w niektórych przypadkach możesz chcieć wymusić uruchomienie synchronizacji dla określonego urządzenia. Możesz uruchomić wymuszoną synchronizację dla następujących urządzeń:

- Urządzenia, na których jest zainstalowany Agent sieciowy
- Urządzenia działające pod kontrolą systemu operacyjnego KasperskyOS

  Przed uruchomieniem wymuszonej synchronizacji dla urządzenia KasperskyOS upewnij się, że urządzenie znajduje się w obszarze punktu dystrybucji oraz że serwer push jest włączony na punkcie dystrybucji.
- Urządzenia iOS
- Urządzenia Android

Przed uruchomieniem wymuszonej synchronizacji dla urządzenia Android musisz skonfigurować Google Firebase Cloud Messaging.

Synchronizowanie pojedynczego urządzenia

W celu wymuszenia synchronizacji między Serwerem administracyjnym a zarządzanym urządzeniem:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.
2. Kliknij nazwę urządzenia, które chcesz zsynchronizować z Serwerem administracyjnym.

   Zostanie otwarte okno właściwości na wybranej sekcji **Ogólne**.
3. Kliknij przycisk **Wymuś synchronizację**.

Aplikacja synchronizuje wybrane urządzenie z Serwerem administracyjnym.

Synchronizowanie kilku urządzeń

W celu wymuszenia synchronizacji między Serwerem administracyjnym a kilkoma zarządzanymi urządzeniami:

1. Otwórz listę urządzeń grupy administracyjnej lub wyboru urządzeń:
   - W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia** → **Grupy**, a następnie wybierz grupę administracyjną, która zawiera urządzenia do synchronizacji.
   - Uruchom wybór urządzeń, aby przejrzeć listę urządzeń.
2. Zaznacz pola obok urządzeń, które chcesz zsynchronizować z Serwerem administracyjnym.
3. Kliknij przycisk **Wymuś synchronizację**.

   Aplikacja synchronizuje wybrane urządzenia z Serwerem administracyjnym.
4. Na liście urządzeń sprawdź, czy czas ostatniego połączenia z Serwerem administracyjnym uległ zmianie dla wybranych urządzeń na bieżący czas. Jeśli czas nie został zmieniony, wówczas zmień zawartość strony, klikając przycisk **Odśwież**.

Wybrane urządzenia zostaną zsynchronizowane z Serwerem administracyjnym.

Przeglądanie czasu dostarczenia zasady

Po zmianie zasady dla aplikacji Kaspersky na Serwerze administracyjnym, administrator może sprawdzić, czy zmieniona zasada została dostarczona do określonego zarządzanego urządzenia. Zasada może zostać dostarczona podczas regularnej synchronizacji lub wymuszonej synchronizacji.

W celu sprawdzenia daty i godziny dostarczenia zasady aplikacji na zarządzane urządzenie:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.
2. Kliknij nazwę urządzenia, które chcesz zsynchronizować z Serwerem administracyjnym.

   Zostanie otwarte okno właściwości na wybranej sekcji **Ogólne**.
3. Wybierz zakładkę **Aplikacje**.

4. Wybierz aplikację, dla której chcesz sprawdzić datę synchronizacji profilu.

   Zostanie otwarte okno zasady aplikacji na sekcji **Ogólne** i z wyświetloną datą i godziną dostarczenia zasady.

Włączanie serwera push

W Kaspersky Security Center punkt dystrybucji może działać jako serwer push dla urządzeń zarządzanych za pośrednictwem protokołu mobilnego oraz zarządzanych za pośrednictwem agenta sieciowego. Na przykład, serwer push musi być włączony, jeśli chcesz mieć możliwość wymuszenia synchronizacji urządzeń KasperskyOS z Serwerem administracyjnym. Serwer push posiada ten sam obszar zarządzanych urządzeń jako punkt dystrybucji, na którym włączono serwer push. Jeśli posiadasz kilka punktów dystrybucji przypisanych dla tej samej grupy administracyjnej, możesz włączyć serwer push na każdym punkcie dystrybucji. W tym przypadku Serwer administracyjny rozkłada obciążenie między punkty dystrybucji.

Punktów dystrybucji można używać jako serwerów push, aby zapewnić ciągłą łączność między zarządzanym urządzeniem a Serwerem administracyjnym. W przypadku niektórych operacji, takich jak uruchamianie i zatrzymywanie zadań lokalnych, odbieranie statystyk dla zarządzanej aplikacji lub tworzenie tunelu, wymagana jest ciągła łączność. Jeśli używasz punktu dystrybucji jako serwera push, nie musisz używać opcji **Nie odłączaj od Serwera administracyjnego** na zarządzanych urządzeniach lub wysyłaj pakiety do portu UDP Agenta sieciowego.

Serwer push obsługuje do 50 000 jednoczesnych połączeń.

W celu włączenia serwera push na punkcie dystrybucji:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Punkty dystrybucji**.

3. Kliknij nazwę punktu dystrybucji, na którym chcesz włączyć serwer push.

   Spowoduje to otwarcie okna właściwości punktu dystrybucji.

4. W sekcji **Ogólne** włącz opcję **Uruchom serwer push**.

5. W polu **Port serwera push** wpisz numer portu. Możesz określić numer dowolnego zajętego portu.

6. W polu **Adres zdalnych hostów** określ adres IP lub nazwę urządzenia punktu dystrybucyjnego.

7. Kliknij przycisk **OK**.

Serwer push jest włączony na wybranym punkcie dystrybucyjnym.

Zarządzanie aplikacjami firm trzecich na urządzeniach klienckich

Ta sekcja opisuje funkcje Kaspersky Security Center, które dotyczą zarządzania aplikacjami firm trzecich zainstalowanymi na urządzeniach klienckich.

Informacje o aplikacjach innych firm

Kaspersky Security Center może pomóc w aktualizacji oprogramowania firm trzecich, zainstalowanego na urządzeniach klienckich, a także w eliminacji luk w oprogramowaniu firm trzecich. Kaspersky Security Center może aktualizować oprogramowanie innych firm tylko z bieżącej wersji do najnowszej wersji. Poniższa lista przedstawia oprogramowanie innych firm, które możesz zaktualizować za pomocą Kaspersky Security Center:

Listę oprogramowania firm trzecich można aktualizować i rozszerzać o nowe aplikacje. Możesz sprawdzić, czy możesz zaktualizować oprogramowanie innych firm (zainstalowane na urządzeniach użytkowników) za pomocą Kaspersky Security Center poprzez przejrzenie listy dostępnych aktualizacji w Kaspersky Security Center Web Console.

- 7-Zip Developers: 7-Zip
- Adobe Systems:
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC
  - Adobe Acrobat
  - Adobe Reader
  - Adobe Shockwave Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander
- Apache Software Foundation: Apache Tomcat
- Apple:
  - Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.: Armory
- Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber
- Code Sector: TeraCopy
- Codec Guide:
  - K-Lite Codec Pack Basic

    - K-Lite Codec Pack Full
    - K-Lite Codec Pack Mega
    - K-Lite Codec Pack Standard
- DbVis Software AB: DbVisualizer
- Decho Corp.:
    - Mozy Enterprise
    - Mozy Home
    - Mozy Pro
- Dominik Reichl: KeePass Password Safe
- Don HO don.h@free.fr: Notepad++
- DoubleGIS: 2GIS
- Dropbox, Inc.: Dropbox
- EaseUs: EaseUS Todo Backup Free
- Electrum Technologies GmbH: Electrum
- Enter Srl: Iperius Backup
- Eric Lawrence: Fiddler
- EverNote: EverNote
- Exodus Movement Inc: Exodus
- EZB Systems: UltraISO
- Famatech:
    - Radmin
    - Remote Administrator
- Far Manager: FAR Manager
- FastStone Soft: FastStone Image Viewer
- Projekt FileZilla: FileZilla
- Firebird Developers: Firebird
- Foxit Corporation:
    - Foxit Reader

    - Foxit Reader Enterprise
- Free Download Manager.ORG: bezpłatny menedżer pobierania
- GIMP project: GIMP
- GlavSoft LLC.: TightVNC
- GNU Project: Gpg4win
- Google:
    - Google Earth
    - Google Chrome
    - Google Chrome Enterprise
    - Google Earth Pro
- Inkscape Project: Inkscape
- IrfanView: IrfanView
- iterate GmbH: Cyberduck
- Logitech: SetPoint
- LogMeIn, Inc.:
    - LogMeIn
    - Hamachi
    - LogMeIn Rescue Technician Console
- Martin Prikryl: WinSCP
- Mozilla Foundation:
    - Mozilla Firefox
    - Mozilla Firefox ESR
    - Mozilla SeaMonkey
    - Mozilla Thunderbird
- New Cloud Technologies Ltd: MyOffice Standard. Edycja domowa
- OpenOffice.org: OpenOffice
- Open Whisper Systems: Signal
- Opera Software: Opera

- Oracle Corporation:
  - Oracle Java JRE
  - Oracle VirtualBox
- PDF44: PDF24 MSI/EXE
- Piriform:
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql: PostgreSQL
- RealNetworks: RealPlayer Cloud
- RealVNC:
  - RealVNC Server
  - RealVNC Viewer
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Pełna/Minimum)
- Simon Tatham: PuTTY
- Skype Technologies: Skype for Windows
- Sober Lemur S.a.s.:
  - PDFsam Basic
  - PDFsam Visual
- Softland: FBackup
- Splashtop Inc.: Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP
- Sublime HQ Pty Ltd: Sublime Text
- TeamViewer GmbH:
  - TeamViewer Host
  - TeamViewer
- Telegram Messenger LLP: Telegram Desktop

- The Document Foundation:
  - LibreOffice
  - LibreOffice HelpPack
- The Git Development Community:
  - Git for Windows
  - Git LFS
- The Pidgin developer community: Pidgin
- TortoiseSVN Developers: TortoiseSVN
- VideoLAN: VLC media player
- VMware:
  - VMware Player
  - VMware Workstation
- WinRAR Developers: WinRAR
- WinZip: WinZip
- Wireshark Foundation: Wireshark
- Wrike: Wrike
- Zimbra: Zimbra Desktop

Instalowanie aktualizacji oprogramowania firm trzecich

Ta sekcja opisuje funkcje Kaspersky Security Center, które dotyczą instalacji aktualizacji dla aplikacji firm trzecich zainstalowanych na urządzeniach klienckich.

Scenariusz: Aktualizowanie oprogramowania innej firmy

Ta sekcja oferuje scenariusz aktualizacji oprogramowania innej firmy, zainstalowanego na urządzeniach klienckich. Oprogramowanie firm trzecich obejmuje aplikacje firmy Microsoft oraz programy innych firm. Aktualizacje dla aplikacji firmy Microsoft są dostarczane przez usługę Windows Update.

Wymagania wstępne

Serwer administracyjny musi mieć połączenie z Internetem, aby zainstalować aktualizacje oprogramowania firm trzecich innego niż oprogramowanie firmy Microsoft.

Domyślnie połączenie internetowe w przypadku Serwera administracyjnego nie jest wymagane w celu instalowania aktualizacji oprogramowania firmy Microsoft na zarządzanych urządzeniach. Na przykład zarządzane urządzenia mogą pobierać aktualizacje oprogramowania firmy Microsoft bezpośrednio z serwerów Microsoft Update lub z systemu Windows Server z programem Microsoft Windows Server Update Services (WSUS) wdrożonymi w sieci organizacji. Serwer administracyjny musi być połączony z Internetem, jeśli jest on używany jako serwer WSUS.

Etapy

Aktualizowanie oprogramowania firm trzecich odbywa się w etapach:

1. **Wyszukiwanie wymaganych aktualizacji**

   Aby odnaleźć aktualizacje oprogramowania firm trzecich dla zarządzanych urządzeń, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

   Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Serwera administracyjnego. Jeśli nie uruchomiono kreatora, utwórz zadanie lub uruchom Kreator wstępnej konfiguracji teraz.

   Dostępne instrukcje:

   - Konsola administracyjna: Skanowanie aplikacji w poszukiwaniu luk, Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console: Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji, Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

2. **Analizowanie listy wykrytych aktualizacji**

   Przejrzyj listę **Aktualizacje oprogramowania** i zdecyduj, które aktualizacje chcesz zainstalować. Aby przejrzeć szczegółowe informacje o każdej aktualizacji, kliknij nazwę aktualizacji na liście. Dla każdej aktualizacji na liście możesz także przejrzeć statystyki dotyczące instalacji aktualizacji na urządzeniach klienckich.

   Dostępne instrukcje:

   - Konsola administracyjna: Przeglądanie informacji o dostępnych aktualizacjach
   - Kaspersky Security Center Web Console: Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

3. **Konfigurowanie instalacji aktualizacji**

   Jeśli Kaspersky Security Center odebrał listę aktualizacji oprogramowania firm trzecich, możesz zainstalować je na urządzeniach klienckich przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki* lub zadania *Zainstaluj aktualizacje Windows Update*. Utwórz jedno z tych zadań. Możesz utworzyć te zadania na zakładce **Zadania** lub korzystając z listy **Aktualizacje oprogramowania**.

   Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do zainstalowania aktualizacji dla aplikacji firmy Microsoft, w tym aktualizacji dostarczonych przez usługę Windows Update, a także aktualizacji produktów innych producentów. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami.

   Zadanie *Zainstaluj aktualizacje Windows Update* nie wymaga licencji, ale może zostać użyte tylko do zainstalowania aktualizacji Windows Update.

   Aby zainstalować niektóre aktualizacje oprogramowania, należy zaakceptować Umowę licencyjną do zainstalowania oprogramowania. Jeśli odrzucisz Umowę licencyjną, aktualizacja oprogramowania nie zostanie zainstalowana.

Możesz uruchomić zadanie instalacji aktualizacji zgodnie z terminarzem. Podczas określania terminarza zadania upewnij się, że zadanie instalacji aktualizacji jest uruchamiane po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

Dostępne instrukcje:

- Konsola administracyjna: Naprawianie luk w aplikacjach, Przeglądanie informacji o dostępnych aktualizacjach
- Kaspersky Security Center Web Console: Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki, Tworzenie zadania Zainstaluj aktualizacje Windows Update, Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

4 **Konfigurowanie terminarza zadań**

Aby upewnić się, że lista aktualizacji jest zawsze aktualna, skonfiguruj terminarz zadania *Wyszukiwanie luk i wymaganych aktualizacji* tak, aby było uruchamiane automatycznie od czasu do czasu. Domyślna częstotliwość uruchamiania to raz na tydzień.

Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej. Podczas konfigurowania terminarza zadania *Zainstaluj aktualizacje Windows Update* należy pamiętać, że dla tego zadania konieczne jest zdefiniowanie listy aktualizacji za każdym razem przed uruchomieniem tego zadania.

Jeśli konfigurujesz terminarz uruchamiania zadań, upewnij się, że zadanie instalacji aktualizacji zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5 **Zatwierdzanie i odrzucanie aktualizacji oprogramowania (opcjonalne)**

Jeśli utworzyłeś zadanie Zainstaluj wymagane aktualizacje i napraw luki, możesz określić reguły instalacji aktualizacji we właściwościach zadania. Jeśli utworzyłeś zadanie Zainstaluj aktualizacje Windows Update, pomiń ten krok.

Dla każdej reguły możesz zdefiniować aktualizacje do zainstalowania w zależności od stanu aktualizacji: *Nie zdefiniowano*, *Zatwierdzono* lub *Odrzucono*. Na przykład, możesz utworzyć określone zadanie dla serwerów i ustawić regułę dla tego zadania, aby zezwolić na instalację tylko aktualizacji Windows Update i tylko tych, które posiadają stan *Zatwierdzono*. Po ręcznym ustawieniu stanu *Zatwierdzono* dla tych aktualizacji, które chcesz zainstalować. W tym przypadku aktualizacje Windows Update, które posiadają stan *Nie zdefiniowano* lub *Odrzucono*, nie będą zainstalowane na serwerach, które określiłeś w zadaniu.

Używanie stanu *Zatwierdzone* do zarządzania instalacją aktualizacji jest wystarczające dla małej ilości uaktualnień. Aby zainstalować kilka aktualizacji, użyj reguł, które możesz skonfigurować w zadaniu *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzone* tylko dla tych określonych aktualizacji, które nie spełniają kryteriów określonych w regułach. Jeśli ręcznie zatwierdzisz dużą liczbę aktualizacji, wydajność Serwera administracyjnego ulegnie zmniejszeniu i może doprowadzić do przeciążenia Serwera administracyjnego.

Domyślnie pobrane uaktualnienia oprogramowania posiadają stan *Niezdefiniowane*. Możesz zmienić stan na *Zatwierdzono* lub *Odrzucono* na liście **Aktualizacje oprogramowania** list (**Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**).

Dostępne instrukcje:

- Konsola administracyjna: Zatwierdzanie i odrzucanie aktualizacji oprogramowania
- Kaspersky Security Center Web Console: Zatwierdzanie i odrzucanie aktualizacji oprogramowania innych firm

6 **Konfigurowanie Serwera administracyjnego do pracy jako serwer Windows Server Update Services (WSUS) (opcjonalne)**

Domyślnie, aktualizacje Windows Update są pobierane na zarządzane urządzenia z serwerów Microsoft. Możesz zmienić to ustawienie, żeby używać Serwera administracyjnego jako serwera WSUS. W tym przypadku Serwer administracyjny synchronizuje dane aktualizacji z Windows Update w określonej częstotliwości i dostarcza aktualizacje w trybie scentralizowanym do Windows Update na urządzeniach w sieci.

Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie Wykonaj synchronizację Windows Update i zaznacz pole **Użyj Serwera administracyjnego jako serwera WSUS** w zasadzie Agenta sieciowego.

Dostępne instrukcje:

- Konsola administracyjna: Synchronizowanie aktualizacji z Windows Update z Serwerem administracyjnym, Konfigurowanie aktualizacji systemu Windows w zasadzie Agenta sieciowego
- Kaspersky Security Center Web Console: Tworzenie zadania synchronizacji Windows Update

7. **Uruchamianie zadania instalacji aktualizacji**

   Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Zainstaluj aktualizacje Windows Update*. Jeśli uruchamiasz te zadania, aktualizacje są pobierane i instalowane na zarządzanych urządzeniach. Po zakończeniu zadania, upewnij się, że na liście zadań posiada stan *Zakończone pomyślnie*.

8. **Utwórz raport dotyczący wyników instalacji aktualizacji oprogramowania firm trzecich (opcjonalne)**

   Aby wyświetlić szczegółowe statystyki dotyczące instalacji aktualizacji, utwórz **Raport z wynikami instalacji aktualizacji oprogramowania firm trzecich**.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie i przeglądanie raportu
   - Kaspersky Security Center Web Console: Tworzenie i przeglądanie raportu

Wyniki

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, aktualizacje są automatycznie instalowane na zarządzanych urządzeniach. Jeśli nowe aktualizacje zostaną pobrane do repozytorium Serwera administracyjnego, Kaspersky Security Center sprawdzi, czy spełniają kryteria określone w regułach aktualizacji. Wszystkie nowe aktualizacje, które spełniają kryteria, zostaną zainstalowane automatycznie przy kolejnym uruchomieniu zadania.

Jeśli utworzyłeś zadanie *Zainstaluj aktualizacje Windows Update*, instalowane są tylko te aktualizacje określone we właściwościach zadania *Zainstaluj aktualizacje Windows Update*. W przyszłości, jeśli będziesz chciał zainstalować nowe aktualizacje pobrane do repozytorium Serwera administracyjnego, będziesz musiał dodać wymagane aktualizacje do listy aktualizacji w istniejącym zadaniu lub utworzyć nowe zadanie *Zainstaluj aktualizacje Windows Update*.

Informacje o aktualizacjach oprogramowania firm trzecich

Kaspersky Security Center umożliwia zarządzanie aktualizacjami oprogramowania firm trzecich, zainstalowanego na zarządzanych urządzeniach, oraz wyeliminowanie luk w aplikacjach Microsoft i produktach innych dostawców poprzez zainstalowanie żądanych aktualizacji.

Kaspersky Security Center wyszukuje aktualizacje za pośrednictwem zadania *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Serwer administracyjny pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania. Po przejrzeniu informacji o dostępnych aktualizacjach, możesz zainstalować je na urządzeniach.

Kaspersky Security Center aktualizuje niektóre aplikacje poprzez usunięcie poprzedniej wersji aplikacji i instalację nowej.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu złośliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk w zabezpieczeniach (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Zadania instalacji aktualizacji oprogramowania firm trzecich

Jeśli metadane aktualizacji oprogramowania firm trzecich są pobierane do repozytorium, możesz zainstalować aktualizacje na urządzeniach klienckich, korzystając z następujących zadań:

- Zadanie *Zainstaluj wymagane aktualizacje i napraw luki*

  Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do zainstalowania aktualizacji dla aplikacji firmy Microsoft, w tym aktualizacji dostarczonych przez usługę Windows Update, a także aktualizacji produktów innych producentów. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami.

  Jeśli to zadanie zostanie zakończone, aktualizacje zostaną automatycznie zainstalowane na zarządzanych urządzeniach. Jeśli metadane nowych aktualizacji zostaną pobrane do repozytorium Serwera administracyjnego, Kaspersky Security Center sprawdzi, czy aktualizacje spełniają kryteria określone w regułach aktualizacji. Wszystkie nowe aktualizacje, które spełniają kryteria, zostaną pobrane i zainstalowane automatycznie przy kolejnym uruchomieniu zadania.

- Zadanie *Zainstaluj aktualizacje Windows Update*

  Zadanie *Zainstaluj aktualizacje Windows Update* nie wymaga licencji, ale może zostać użyte tylko do zainstalowania aktualizacji Windows Update.

  Jeśli to zadanie zostanie zakończone, zostaną zainstalowane tylko te aktualizacje, które zostały określone we właściwościach zadania. W przyszłości, jeśli będziesz chciał zainstalować nowe aktualizacje pobrane do repozytorium Serwera administracyjnego, będziesz musiał dodać wymagane aktualizacje do listy aktualizacji w istniejącym zadaniu lub utworzyć nowe zadanie Zainstaluj aktualizacje Windows Update.

Używanie Serwera administracyjnego jako serwera WSUS

Informacje o aktualizacjach dostępnych dla Microsoft Windows są dostępne poprzez usługę Windows Update. Serwer administracyjny może zostać użyty jako serwer Windows Server Update Services (WSUS). Aby użyć Serwera administracyjnego jako serwera WSUS, utwórz zadanie Wykonaj synchronizację Windows Update i wybierz opcję **Użyj Serwera administracyjnego jako serwera WSUS** w zasadzie Agenta sieciowego. Po skonfigurowaniu synchronizacji danych z Windows Update, Serwer administracyjny zapewnia aktualizacje dla usług Windows Update na urządzeniach w trybie scentralizowanym i z określoną częstotliwością.

Instalowanie aktualizacji oprogramowania firm trzecich

Możesz zainstalować aktualizacje oprogramowania firm trzecich na zarządzanych urządzeniach poprzez stworzenie i uruchomienie jednego z następujących zadań:

- *Zainstaluj wymagane aktualizacje i napraw luki*

  Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami. Możesz użyć tego zadania, aby zainstalować aktualizacje Windows Update dostarczone przez Microsoft oraz aktualizacje dla produktów innych producentów.

- *Zainstaluj aktualizacje Windows*

  Możesz użyć zadania *Zainstaluj aktualizacje Windows* tylko do zainstalowania aktualizacji Windows Update.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Opcjonalnie możesz utworzyć zadanie instalacji wymaganych aktualizacji w następujący sposób:

- Otwierając listę aktualizacji i określając aktualizacje do zainstalowania.

  W rezultacie tworzone jest nowe zadanie instalacji wybranych aktualizacji. Istnieje możliwość dodania wybranych aktualizacji do istniejącego zadania.

- Uruchamiając kreator instalacji aktualizacji.

  kreator instalacji aktualizacji jest dostępny tylko dla licencji Zarządzanie lukami i poprawkami.

  Kreator upraszcza tworzenie i konfigurację zadania instalacji aktualizacji i pozwala wyeliminować tworzenie zbędnych zadań zawierających te same aktualizacje do zainstalowania.

Instalowanie aktualizacji oprogramowania innych firm przy użyciu listy aktualizacji

W celu zainstalowania aktualizacji dla oprogramowania firm trzecich, korzystając z listy aktualizacji:

1. Otwórz jedną z list aktualizacji:

   - Aby otworzyć ogólną listę aktualizacji, przejdź do **Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.
   - Aby otworzyć listę aktualizacji dla zarządzanego urządzenia, przejdź do **Urządzenia** → **Zarządzane urządzenia** → <device name> → **Zaawansowane** → **Dostępne aktualizacje**.
   - Aby otworzyć listę aktualizacji dla określonej aplikacji, przejdź do **Operacje** → **Aplikacje innych firm** → **Rejestr aplikacji** → <application name> → **Dostępne aktualizacje**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

2. Zaznacz pola obok aktualizacji, które chcesz zainstalować.

3. Kliknij przycisk **Zainstaluj aktualizacje**.

   Aby zainstalować niektóre aktualizacje oprogramowania, należy zaakceptować Umowę licencyjną. Jeśli odrzucisz Umowę licencyjną, aktualizacja oprogramowania nie zostanie zainstalowana.

4. Wybierz jedną z następujących opcji:

   - **Nowe zadanie**

     Zostanie uruchomiony Kreator tworzenia nowego zadania. Jeśli masz licencję Zarządzania lukami i poprawkami, domyślnie wybrany jest typ zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Jeśli nie masz licencji, wybrane jest zadanie *Zainstaluj aktualizacje Windows*. Aby zakończyć tworzenie zadania, postępuj zgodnie z instrukcjami kreatora.

   - **Zainstaluj aktualizację (dodaj regułę do określonego zadania)**

     Wybierz zadanie, do którego chcesz dodać wybrane aktualizacje. Jeśli masz licencję Zarządzania lukami i poprawkami, wybierz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*. Nowa reguła instalacji wybranych aktualizacji zostanie automatycznie dodana do wybranego zadania. Jeśli nie masz licencji, wybierz zadanie *Zainstaluj aktualizacje Windows*. Wybrane aktualizacje zostaną dodane do właściwości zadania.

     Zostanie otwarte okno właściwości zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Jeśli wybrałeś utworzenie nowego zadania, zadanie zostanie utworzone i wyświetlone na liście zadań, w sekcji **Urządzenia → Zadania**. Jeśli wybrałeś dodanie aktualizacji do istniejącego zadania, aktualizacje zostaną zapisane we właściwościach zadania.

Aby zainstalować aktualizacje dla oprogramowania innych firm, uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Zainstaluj aktualizacje Windows*. Możesz uruchomić jakiekolwiek z tych zadań ręcznie lub określić ustawienia terminarza we właściwościach zadania, które uruchomiłeś. Podczas określania terminarza zadania upewnij się, że zadanie instalacji aktualizacji jest uruchamiane po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

Instalowanie aktualizacji oprogramowania innych firm za pomocą Kreator naprawiania luk

kreator instalacji aktualizacji jest dostępny tylko dla licencji Zarządzanie lukami i poprawkami.

W celu utworzenia zadania instalacji aktualizacji oprogramowania firm trzecich, korzystając z Kreator naprawiania luk:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Aktualizacje oprogramowania**.

   Zostanie wyświetlona lista dostępnych aktualizacji.

2. Zaznacz pole obok aktualizacji, którą chcesz zainstalować.

3. Kliknij przycisk **Uruchom kreatora instalacji aktualizacji**.

   Zostanie uruchomiony kreator instalacji aktualizacji. Strona **Wybierz zadanie instalacji aktualizacji** wyświetla listę wszystkich istniejących zadań następujących typów:

   - *Zainstaluj wymagane aktualizacje i napraw luki*
   - *Zainstaluj aktualizacje Windows*
   - *Napraw luki*

   Nie możesz zmodyfikować zadań ostatnich dwóch typów, aby zainstalować nowe aktualizacje. Aby zainstalować nowe aktualizacje, możesz użyć tylko zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

4. Jeśli chcesz, aby kreator wyświetlał tylko te zadania, które instalują wybraną aktualizację, włącz opcję **Wyświetl tylko zadania instalujące tę aktualizację**.

5. Wybierz, co chcesz zrobić:

- Aby rozpocząć zadanie, zaznacz pole wyboru obok nazwy zadania, a następnie kliknij przycisk **Uruchom**.
- Aby dodać nową regułę do istniejącego zadania:

  a. Zaznacz pole obok nazwy zadania i kliknij przycisk **Dodaj regułę**.

  b. Na wyświetlonej stronie skonfiguruj nową regułę:

  - Reguła instalacji dla aktualizacji tej istotności

    Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

    Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

    Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

    Domyślnie opcja ta jest wyłączona.

  - Reguła instalacji aktualizacji tej istotności zgodnie z MSRC

    Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

    Jeśli ta opcja jest włączona (dostępna tylko dla aktualizacji systemu Windows Update), aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

    Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

    Domyślnie opcja ta jest wyłączona.

  - Reguła instalacji dla aktualizacji tego dostawcy

    Ta opcja jest dostępna tylko dla aktualizacji aplikacji innych firm. Kaspersky Security Center instaluje tylko te aktualizacje, które odnoszą się do aplikacji stworzonych przez tego samego dostawcę co wybrana aktualizacja. Odrzucone aktualizacje i aktualizacje aplikacji stworzone przez innych dostawców nie są instalowane.

    Domyślnie opcja ta jest wyłączona.

  - **Reguła instalacji dla aktualizacji typu**
  - **Reguła instalacji dla wybranej aktualizacji**
  - Zatwierdź wybrane aktualizacje

Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

Domyślnie opcja ta jest wyłączona.

- **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

  Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

  Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

  Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

  Domyślnie opcja ta jest włączona.

c. Kliknij przycisk **Dodaj**.

- W celu utworzenia zadania:

  a. Kliknij przycisk **Nowe zadanie**.

  b. Na wyświetlonej stronie skonfiguruj nową regułę:

  - **Reguła instalacji dla aktualizacji tej istotności**

    Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

    Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

    Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

    Domyślnie opcja ta jest wyłączona.

  - **Reguła instalacji aktualizacji tej istotności zgodnie z MSRC**

Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

Jeśli ta opcja jest włączona (dostępna tylko dla aktualizacji systemu Windows Update), aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

Domyślnie opcja ta jest wyłączona.

- **Reguła instalacji dla aktualizacji tego dostawcy**

  Ta opcja jest dostępna tylko dla aktualizacji aplikacji innych firm. Kaspersky Security Center instaluje tylko te aktualizacje, które odnoszą się do aplikacji stworzonych przez tego samego dostawcę co wybrana aktualizacja. Odrzucone aktualizacje i aktualizacje aplikacji stworzone przez innych dostawców nie są instalowane.

  Domyślnie opcja ta jest wyłączona.

- **Reguła instalacji dla aktualizacji typu**
- **Reguła instalacji dla wybranej aktualizacji**
- **Zatwierdź wybrane aktualizacje**

  Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

  Domyślnie opcja ta jest wyłączona.

- **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

  Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

  Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

  Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

  Domyślnie opcja ta jest włączona.

c. Kliknij przycisk **Dodaj**.

Jeśli wybrano rozpoczęcie zadania, możesz zamknąć kreatora. Zadanie zakończy się w tle. Dalsze działania nie są wymagane.

Jeśli wybrałeś dodanie reguły do istniejącego zadania, zostanie otwarte okno właściwości zadania. Nowa reguła została już dodana do właściwości zadania. Możesz przejrzeć lub zmodyfikować regułę lub ustawienia innego zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Jeśli chcesz utworzyć zadanie, kontynuuj tworzenie zadania w kreatorze tworzenia nowego zadania. Nowa reguła dodana w kreatorze instalacji aktualizacji zostanie wyświetlona w kreatorze tworzenia nowego zadania. Po zakończeniu pracy kreatora, do listy zadań zostanie dodane zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji

Za pośrednictwem zadania Wyszukiwanie luk i wymaganych aktualizacji program Kaspersky Security Center otrzymuje listy wykrytych luk i wymaganych aktualizacji dla oprogramowania firm trzecich, zainstalowanego na zarządzanych urządzeniach.

Zadanie Wyszukiwanie luk i wymaganych aktualizacji jest tworzone automatycznie po uruchomieniu kreatora wstępnej konfiguracji. Jeśli nie uruchamiałeś kreatora, możesz utworzyć zadanie ręcznie.

W celu utworzenia zadania Wyszukiwanie luk i wymaganych aktualizacji:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Wyszukiwanie luk i wymaganych aktualizacji**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
7. Kliknij przycisk **Utwórz**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.
8. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.
9. W oknie właściwości zadania określ ogólne ustawienia zadania.
10. Na zakładce **Ustawienia aplikacji** określ następujące ustawienia:

    - **Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft**

Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

Domyślnie opcja ta jest włączona.

- **Połącz z serwerem aktualizacji, aby zaktualizować dane**

  Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł uaktualnień Microsoft:

  - Serwer administracyjny Kaspersky Security Center (zapoznaj się z ustawieniami profilu Agenta sieciowego)
  - System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
  - Serwery aktualizacji Microsoft

  Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

  Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła uaktualnień Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

  Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach profilu Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

  Domyślnie opcja ta jest włączona.

  Kombinacja następujących opcji ustawień profilu Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

  - Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie z serwerem aktualizacji, aby uzyskać aktualizacje tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona, a opcja **Aktywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została zaznaczona.
  - Agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła uaktualnień Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia, jeśli opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** została włączona, a opcja **Pasywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została wybrana, jeśli opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest wyłączona, a opcja **Aktywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została zaznaczona.
  - Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Wyłączono** w ustawieniach grupy **Tryb wyszukiwania aktualizacji systemu Windows** jest zaznaczona, Kaspersky Security Center nie żąda żadnych informacji o aktualizacjach.

- **Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky**

  Jeśli ta opcja jest włączona, Kaspersky Security Center wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

  Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

- **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**

  Foldery, w których Kaspersky Security Center wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

  Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

11. Kliknij przycisk **Zapisz**.

Zadanie zostało utworzone i skonfigurowane.

Jeśli wyniki zadania zawierają ostrzeżenie o błędzie 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie po uruchomieniu kreatora wstępnej konfiguracji. Jeśli nie uruchamiałeś kreatora, możesz utworzyć zadanie ręcznie.

Oprócz ogólnych ustawień zadania możesz określić następujące ustawienia podczas tworzenia zadania *Wyszukiwanie luk i wymaganych aktualizacji* lub później, podczas konfigurowania właściwości utworzonego zadania:

- **Wyszukaj luki i aktualizacje wymienione przez firmę Microsoft**

  Podczas wyszukiwania luk i aktualizacji program Kaspersky Security Center używa informacji o stosowanych aktualizacjach firmy Microsoft ze źródła uaktualnień Microsoft, które są dostępne w danym momencie.

  Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft i aktualizacji aplikacji innych firm.

  Domyślnie opcja ta jest włączona.

- **Połącz z serwerem aktualizacji, aby zaktualizować dane**

Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem uaktualnień Microsoft. Następujące serwery mogą pełnić rolę źródeł uaktualnień Microsoft:

- Serwer administracyjny Kaspersky Security Center (zapoznaj się z ustawieniami profilu Agenta sieciowego)
- System Windows Server wdrożony w sieci Twojej organizacji wraz z programem Microsoft Windows Server Update Services (WSUS)
- Serwery aktualizacji Microsoft

Jeśli ta opcja jest włączona, agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie ze źródłem aktualizacji firmy Microsoft, aby odświeżyć informacje o stosowanych aktualizacjach Microsoft Windows.

Jeśli ta opcja jest wyłączona, agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła uaktualnień Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia.

Nawiązywanie połączenia ze źródłem aktualizacji firmy Microsoft może zużywać dużo zasobów. Możesz chcieć wyłączyć tę opcję, jeśli ustawisz regularne nawiązywanie połączenia z tym źródłem uaktualnień w innym zadaniu lub we właściwościach profilu Agenta sieciowego, w sekcji **Aktualizacje oprogramowania i luki**. Jeśli nie chcesz wyłączyć tej opcji, następnie, aby zmniejszyć obciążenie Serwera, możesz skonfigurować terminarz zadania do losowego opóźnienia uruchomienia zadania w ciągu 360 minut.

Domyślnie opcja ta jest włączona.

Kombinacja następujących opcji ustawień profilu Agenta sieciowego definiuje tryb uzyskiwania aktualizacji:

- Agent usługi Windows Update na zarządzanym urządzeniu nawiązuje połączenie z serwerem aktualizacji, aby uzyskać aktualizacje tylko wtedy, gdy opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest włączona, a opcja **Aktywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została zaznaczona.
- Agent usługi Windows Update na zarządzanym urządzeniu używa informacji o stosowanych aktualizacjach Microsoft Windows, które zostały pobrane ze źródła uaktualnień Microsoft wcześniej i które są przechowywane w pamięci podręcznej urządzenia, jeśli opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** została włączona, a opcja **Pasywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została wybrana, jeśli opcja **Połącz z serwerem aktualizacji, aby zaktualizować dane** jest wyłączona, a opcja **Aktywny** w grupie ustawień **Tryb wyszukiwania aktualizacji systemu Windows** została zaznaczona.
- Bez względu na stan opcji **Połącz z serwerem aktualizacji, aby zaktualizować dane** (włączona lub wyłączona), jeśli opcja **Wyłączono** w ustawieniach grupy **Tryb wyszukiwania aktualizacji systemu Windows** jest zaznaczona, Kaspersky Security Center nie żąda żadnych informacji o aktualizacjach.

- Wyszukaj luki i aktualizacje innych firm wymienione przez firmę Kaspersky

Jeśli ta opcja jest włączona, Kaspersky Security Center wyszukuje luki i wymagane aktualizacje dla aplikacji firm trzecich (aplikacji producentów innych niż Kaspersky i Microsoft) w rejestrze systemu Windows i w folderach określonych pod **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**. Pełna lista obsługiwanych aplikacji firm trzecich jest zarządzana przez Kaspersky.

Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie szuka luk i wymaganych uaktualnień dla aplikacji firm trzecich. Na przykład, możesz chcieć wyłączyć tę opcję, jeśli posiadasz różne zadania z różnymi ustawieniami aktualizacji Microsoft Windows i aktualizacji aplikacji innych firm.

Domyślnie opcja ta jest włączona.

- **Określ ścieżki zaawansowanego wyszukiwania aplikacji w systemie plików**

  Foldery, w których Kaspersky Security Center wyszukuje aplikacje firm trzecich, które wymagają naprawienia luk i zainstalowania aktualizacji. Możesz użyć zmiennych systemowych.

  Określ foldery, w których zostaną zainstalowane aplikacje. Domyślnie, lista zawiera foldery systemowe, w których instalowana jest większość aplikacji.

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

Zalecenia dotyczące terminarza zadania

Podczas tworzenia terminarza zadania *\Wyszukiwanie luk i wymaganych aktualizacji* upewnij się, że włączone są dwie opcje: **Uruchom pominięte zadania** oraz **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Domyślnie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest ustawione do uruchamiania o godzinie 18:00. Jeśli zasady obowiązujące w miejscu pracy wymagają wyłączenia wszystkich urządzeń o tej godzinie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie uruchomione po ponownym włączeniu urządzeń, czyli rano następnego dnia. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemów dysku. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft, zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawę kilku luk zgodnie z pewnymi regułami.

W celu zainstalowania aktualizacji lub wyeliminowania luk za pomocą zadania *Zainstaluj wymagane aktualizacje i napraw luki*, możesz wykonać jedną z następujących czynności:

- Uruchom kreator instalacji aktualizacji lub Kreator naprawiania luk.
- Utwórz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.
- Dodaj regułę instalacji aktualizacji do istniejącego pliku *Zainstaluj wymagane aktualizacje i napraw luki* zadanie.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Zainstaluj wymagane aktualizacje i napraw luki**.

   Jeśli zadanie nie jest wyświetlane, sprawdź, czy Twoje konto ma uprawnienia **Odczyt**, **Modyfikuj** i **Wykonaj** dla obszaru funkcjonalnego **Zarządzanie systemem: Zarządzanie lukami w zabezpieczeniach i poprawkami**. Bez tych praw dostępu nie można utworzyć ani skonfigurować zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Określ zasady instalacji aktualizacji, a następnie określ następujące ustawienia:

   - **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia**

     Jeśli ta opcja jest włączona, aktualizacje są instalowane po ponownym uruchomieniu lub zamknięciu urządzenia. W innym przypadku aktualizacje są instalowane zgodnie z terminarzem.

     Użyj tej opcji, jeśli instalowanie aktualizacji może wpłynąć na działanie urządzenia.

     Domyślnie opcja ta jest wyłączona.

   - **Zainstaluj wymagane ogólne składniki systemu**

     Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

     Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

     Domyślnie opcja ta jest wyłączona.

   - **Zezwól na instalację nowych wersji aplikacji podczas aktualizacji**

Jeśli ta opcja jest włączona, aktualizacje są dozwolone, gdy powodują zainstalowanie nowej wersji aplikacji.

Jeśli ta opcja jest wyłączona, aplikacja nie zostanie zaktualizowana. W takiej sytuacji możesz ręcznie zainstalować nowe wersje aplikacji lub użyć w tym celu innego zadania. Na przykład, możesz użyć tej opcji, jeśli struktura Twojej firmy nie jest obsługiwana przez nową wersję aplikacji lub jeśli chcesz sprawdzić aktualizację w infrastrukturze testowej.

Domyślnie opcja ta jest włączona.

Aktualizowanie aplikacji może spowodować problemy z działaniem powiązanych aplikacji zainstalowanych na urządzeniach klienckich.

- **Pobierz aktualizacje na urządzenie, ale ich nie instaluj**

  Jeśli ta opcja jest włączona, aplikacja pobierze uaktualnienia na urządzenie, ale nie zainstaluje ich automatycznie. Możesz ręcznie zainstalować pobrane aktualizacje.

  Aktualizacje Microsoft są pobierane do folderu systemowego Windows. Aktualizacje aplikacji firm trzecich (aplikacje innych producentów niż Kaspersky i Microsoft) są pobierane do folderu określonego w polu **Folder do pobierania aktualizacji**.

  Jeśli ta opcja jest wyłączona, aktualizacje są instalowane na urządzeniu automatycznie.

  Domyślnie opcja ta jest wyłączona.

- **Folder do pobierania aktualizacji**

  Ten folder jest używany do pobierania aktualizacji aplikacji innych firm (aplikacji innych producentów niż Kaspersky i Microsoft).

- **Włącz diagnostykę zaawansowaną**

  Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

  Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

  Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

  Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

7. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Czas oczekiwania przed wymuszeniem zamknięcia aplikacji dla zablokowanych sesji (min)**

  Wymuszone zamknięcie aplikacji ma miejsce, gdy urządzenie użytkownika jest zablokowane (automatycznie po określonym czasie nieaktywności lub ręcznie).

  Jeśli ta opcja jest włączona, wymuszone zamknięcie aplikacji na zablokowanym urządzeniu odbywa się po minięciu czasu określonego w polu wejściowym.

  Jeśli ta opcja jest wyłączona, aplikacje nie będą zamykane na zablokowanym urządzeniu.

  Domyślnie opcja ta jest wyłączona.

8. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

10. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

11. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

12. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

Jeśli wyniki zadania zawierają ostrzeżenie o błędzie 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

Dodawanie reguł dla instalacji aktualizacji

Ta funkcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

Podczas instalowania aktualizacji oprogramowania lub naprawiania luk w oprogramowaniu przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki* należy określić zasady instalacji aktualizacji. Te reguły określają aktualizacje do zainstalowania oraz luki do wyeliminowania.

Dokładne ustawienia zależą od tego, czy dodajesz regułę dla wszystkich aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich (aplikacje stworzone przez producentów oprogramowania innych niż Kaspersky i Microsoft) lub wszystkich aplikacji. Podczas dodawania reguły dla aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich możesz wybrać określone aplikacje oraz wersje aplikacji, dla których chcesz zainstalować uaktualnienia. Podczas dodawani reguły dla wszystkich aktualizacji możesz wybrać określone uaktualnienia, które chcesz zainstalować, oraz luki, które chcesz wyeliminować poprzez zainstalowanie uaktualnień.

Regułę instalacji aktualizacji można dodać w następujący sposób:

- Dodając regułę podczas tworzenia nowego zadania Zainstaluj wymagane aktualizacje i napraw luki.
- Dodając regułę w zakładce **Ustawienia aplikacji** w oknie właściwości istniejącego zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
- Za pomocą kreatora instalacji aktualizacji lub kreatora naprawiania luk.

W celu dodania nowej reguły dla wszystkich aktualizacji:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla wszystkich aktualizacji**.

3. W kroku **Kryteria ogólne** użyj list rozwijalnych do określenia następujących ustawień:

- **Zbiór uaktualnień do zainstalowania**

  Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

  - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
  - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
  - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

- **Napraw luki z priorytetem równym lub większym niż**

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

4. W kroku **Aktualizacje** wybierz aktualizacje, które mają zostać zainstalowane:

- **Zainstaluj wszystkie pasujące aktualizacje**

  Zainstaluj aktualizacje oprogramowania, które spełniają kryteria określone w kroku **Kryteria ogólne**. Ta opcja jest wybrana domyślnie.

- **Zainstaluj tylko aktualizacje z listy**

  Instalowane są tylko te aktualizacje oprogramowania, które wybierzesz ręcznie z listy. Ta lista zawiera wszystkie dostępne aktualizacje oprogramowania.

  Na przykład, możesz wybrać określone aktualizacje w następujących przypadkach: aby sprawdzić ich instalację w środowisku testowym, aby zaktualizować tylko krytyczne aplikacje lub aby zaktualizować tylko określone aplikacje.

  - **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

Domyślnie opcja ta jest włączona.

5. W kroku **Luki** wybierz luki, które zostaną wyeliminowane poprzez zainstalowanie wybranych aktualizacji:

   - Napraw wszystkie luki spełniające inne kryteria

     Wyeliminuj wszystkie luki, które spełniają kryteria określone na stronie **Kryteria ogólne** kreatora. Ta opcja jest wybrana domyślnie.

   - Napraw tylko luki z listy

     Naprawione zostaną tylko te luki, które ręcznie wybierzesz z listy. Ta lista zawiera wszystkie wykryte luki.

     Na przykład, możesz wybrać określone luki w następujących przypadkach: aby sprawdzić ich eliminację w środowisku testowym, aby wyeliminować luki tylko w krytycznych aplikacjach lub aby wyeliminować luki tylko w określonych aplikacjach.

6. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

W celu dodania nowej reguły dla aktualizacji Windows Update:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji systemu Windows**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - Zbiór uaktualnień do zainstalowania

Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

- **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
- **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
- **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

- Napraw luki z priorytetem równym lub większym niż

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

- Napraw luki z priorytetem MSRC równym lub większym niż

  Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

  Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni, Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

  Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

  Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.
5. W kroku **Kategorie aktualizacji** wybierz kategorie aktualizacji, które mają zostać zainstalowane. Te kategorie są takie same, jak w Microsoft Update Catalog. Domyślnie, zaznaczone są wszystkie kategorie.
6. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

W celu dodania nowej reguły dla aktualizacji aplikacji firm trzecich:

1. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji firm trzecich**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - Zbiór uaktualnień do zainstalowania

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - Napraw luki z priorytetem równym lub większym niż

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji Ustawienia okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

Tworzenie zadania Zainstaluj aktualizacje Windows Update

Zadanie *Zainstaluj aktualizacje Windows* umożliwia zainstalowanie aktualizacji oprogramowania, dostarczonych przez usługę Windows Update na zarządzane urządzenia.

Jeśli nie masz licencji Zarządzania lukami i poprawkami, nie możesz tworzyć nowych zadań typu *Zainstaluj aktualizacje Windows*. Aby zainstalować nowe aktualizacje, możesz dodać je do istniejącego zadania *Zainstaluj aktualizacje Windows*. Zalecamy użycie zadania *Zainstaluj wymagane aktualizacje i napraw luki* zamiast zadania *Zainstaluj aktualizacje Windows*. Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* umożliwia automatyczne instalowanie wielu aktualizacji i naprawianie wielu luk w zabezpieczeniach, zgodnie z określonymi przez Ciebie regułami. Ponadto to zadanie umożliwia instalowanie aktualizacji od dostawców oprogramowania innych niż Microsoft.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

W celu utworzenia zadania Zainstaluj aktualizacje Windows Update:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Zainstaluj aktualizacje Windows**.
4. Określ nazwę tworzonego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Kliknij przycisk **Dodaj**.

   Zostanie otwarta lista aktualizacji.
7. Wybierz aktualizacje Windows Update, które chcesz zainstalować, a następnie kliknij **OK**.
8. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

   - **Nie uruchamiaj ponownie urządzenia**

     Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

   - **Uruchom urządzenie ponownie**

     Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

   - **Pytaj użytkownika o akcję**

Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

  Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

  Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

  Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

  Domyślnie opcja ta jest wyłączona.

9. Określ ustawienia konta:

- **Konto domyślne**

  Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

  Domyślnie opcja ta jest zaznaczona.

- **Określ konto**

  Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

- Konto

  Konto, z poziomu którego zadanie jest uruchamiane.

- Hasło

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

10. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.
11. Kliknij przycisk **Zakończ**.

    Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.
12. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.
13. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.
14. Kliknij przycisk **Zapisz**.

Zadanie zostało utworzone i skonfigurowane.

Przeglądanie informacji o dostępnych aktualizacjach oprogramowania firm trzecich

Możesz przejrzeć listę dostępnych aktualizacji dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, zainstalowanego na urządzeniach klienckich.

W celu przejrzenia listy aktualizacji dostępnych dla aplikacji firm trzecich, zainstalowanych na urządzeniach klienckich:

W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Aktualizacje oprogramowania**.

Zostanie wyświetlona lista dostępnych aktualizacji.

Możesz określić filtr przeglądania listy aktualizacji oprogramowania. Kliknij ikonę **Filtr** ( ) w prawym górnym rogu listy aktualizacji oprogramowania do zarządzania filtrem. Możesz także wybrać jeden z predefiniowanych filtrów z listy rozwijalnej **Wstępnie ustawione filtry** nad listą luk w oprogramowaniu.

W celu przejrzenia właściwości aktualizacji:

1. Kliknij nazwę żądanej aktualizacji oprogramowania.
2. Zostanie otwarte okno właściwości aktualizacji, wyświetlające informacje pogrupowane na następujących zakładkach:

   - Ogólne

Ta zakładka wyświetla ogólne szczegóły wybranej aktualizacji:

- Stan zatwierdzenia aktualizacji (można zmienić ręcznie, wybierają nowy stan na liście rozwijalnej)
- Kategoria Windows Server Update Services (WSUS), do której należy aktualizacja
- Data i godzina zarejestrowania aktualizacji
- Data i godzina utworzenia aktualizacji
- Istotność aktualizacji
- Wymagania instalacyjne: nałożone przez aktualizację
- Rodzina aplikacji, do której należy aktualizacja
- Aplikacja, do której stosowana jest aktualizacja
- Liczba rewizji aktualizacji

- **Atrybuty**

  Ta zakładka wyświetla zestaw atrybutów, których możesz użyć do uzyskania większej ilości informacji na temat wybranej aktualizacji. Ten zestaw różni się w zależności od tego, czy aktualizacja jest publikowana przez firmę Microsoft lub innego producenta.

  Zakładka wyświetla następujące informacje dla aktualizacji firmy Microsoft:

  - Poziom ważności aktualizacji zgodny z Microsoft Security Response Center (MSRC)
  - Odnośnik do artykułu w Bazie wiedzy Microsoft Knowledge Base opisujący aktualizację
  - Odnośnik do artykułu w biuletynie Microsoft Security Bulletin opisujący aktualizację
  - Identyfikator aktualizacji (ID)

  Zakładka wyświetla następujące informacje dla aktualizacji innej firmy:

  - Czy aktualizacja jest poprawką lub pełnym pakietem dystrybucyjnym
  - Język lokalizacji aktualizacji
  - Czy aktualizacja jest instalowana automatycznie lub ręcznie
  - Czy aktualizacja została wycofana po zastosowaniu
  - Odnośnik do pobrania aktualizacji

- **Urządzenia**

  Ta zakładka wyświetla listę urządzeń, na których zainstalowano wybraną aktualizację.

- **Naprawione luki**

Ta zakładka wyświetla listę luk, które mogą zostać usunięte przez wybraną aktualizację.

- **Podział aktualizacji**

  Ta zakładka wyświetla możliwe podziały między różnymi aktualizacjami opublikowanymi dla tej samej aplikacji, czyli czy wybrana aktualizacja może zastąpić inne aktualizacje lub czy mogą zostać zastąpione przez inne aktualizacje (dostępne tylko dla aktualizacji Microsoft).

- **Zadania instalacji tej aktualizacji**

  Ta zakładka wyświetla listę zadań, których obszar obejmuje instalację wybranej aktualizacji. Zakładka umożliwia także utworzenie nowego zadania zdalnej instalacji dla aktualizacji.

W celu przejrzenia statystyk dotyczących instalacji aktualizacji:

1. Zaznacz pole obok żądanej aktualizacji oprogramowania.
2. Kliknij przycisk **Statystyki stanów instalacji aktualizacji**.

   Zostanie wyświetlony wykres stanów instalacji aktualizacji. Kliknięcie stanu spowoduje otwarcie listy urządzeń, na których aktualizacja posiada wybrany stan.

Możesz przejrzeć informacje o dostępnych aktualizacjach oprogramowania dla programów firm trzecich, w tym programów firmy Microsoft, zainstalowanych na wybranym zarządzanym urządzeniu działającym pod kontrolą systemu Windows.

W celu przejrzenia listy aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanych na wybranych zarządzanych urządzeniach:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, dla którego chcesz przejrzeć aktualizacje oprogramowania firm trzecich.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.

3. W oknie właściwości wybranego urządzenia wybierz zakładkę **Zaawansowane**.
4. W lewej części okna wybierz sekcję **Dostępne aktualizacje**. Jeśli chcesz przejrzeć tylko zainstalowane aktualizacje, włącz opcję **Pokaż zainstalowane aktualizacje**.

   Zostanie wyświetlona lista aktualizacji oprogramowania firm trzecich, dostępnych dla wybranego urządzenia.

Eksportowanie listy dostępnych aktualizacji oprogramowania do pliku

Możesz wyeksportować aktualizacje dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, które jest aktualnie wyświetlane, do plików CSV lub TXT. Możesz użyć tych plików, na przykład, do wysłania ich do swojego menedżera ds. bezpieczeństwa informacji lub przechowywać je w celach statystycznych.

W celu wyeksportowania do pliku tekstowego listy aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanego na wszystkich zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Aktualizacje oprogramowania**.

   Strona wyświetla listę aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanego na wszystkich zarządzanych urządzeniach.

2. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj wiersze do pliku TXT** lub przycisk **Eksportuj wiersze do pliku CSV**.

Plik zawierający listę aktualizacji dostępnych dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, zostanie pobrany na urządzenie, którego aktualnie używasz.

W celu wyeksportowania do pliku tekstowego listy aktualizacji dostępnych dla oprogramowania firm trzecich, zainstalowanego na wybranym zarządzanym urządzeniu:

1. Otwórz listę aktualizacji dostępnych dla oprogramowania firm trzecich na wybranym, zarządzanym urządzeniu.

2. Wybierz aktualizacje oprogramowania, które chcesz wyeksportować.

   Pomiń ten krok, jeśli chcesz wyeksportować pełną listę aktualizacji oprogramowania.

   Jeśli chcesz wyeksportować pełną listę aktualizacji oprogramowania, zostaną wyeksportowane tylko aktualizacje wyświetlające bieżącą stronę.

   Jeśli chcesz wyeksportować tylko zainstalowane aktualizacje, zaznacz pole **Pokaż zainstalowane aktualizacje**.

3. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj wiersze do pliku TXT** lub przycisk **Eksportuj wiersze do pliku CSV**.

Plik zawierający listę aktualizacji dla oprogramowania firm trzecich, w tym oprogramowania firmy Microsoft, zainstalowanego na wybranym, zarządzanym urządzeniu, jest pobierany na aktualnie używane urządzenie.

Zatwierdzanie oraz odrzucanie aktualizacji oprogramowania firm trzecich

Jeśli konfigurujesz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz utworzyć regułę, która wymaga określonego stanu aktualizacji, które zostaną zainstalowane. Na przykład, reguła aktualizacji może zezwolić na instalację następujących elementów:

- Tylko zatwierdzonych aktualizacji
- Tylko zatwierdzonych i niezdefiniowanych aktualizacji
- Wszystkich aktualizacji niezależnie od stanu aktualizacji

Możesz zatwierdzić uaktualnienia, które muszą zostać zainstalowane, oraz odrzucić uaktualnienia, które nie muszą zostać zainstalowane.

Używanie stanu *Zatwierdzone* do zarządzania instalacją aktualizacji jest wystarczające dla małej ilości uaktualnień. Aby zainstalować kilka aktualizacji, użyj reguł, które możesz skonfigurować w zadaniu *Zainstaluj wymagane aktualizacje i napraw luki*. Zalecane jest ustawienie stanu *Zatwierdzone* tylko dla tych określonych aktualizacji, które nie spełniają kryteriów określonych w regułach. Jeśli ręcznie zatwierdzisz dużą liczbę aktualizacji, wydajność Serwera administracyjnego ulegnie zmniejszeniu i może doprowadzić do przeciążenia Serwera administracyjnego.

W celu zatwierdzenia lub odrzucenia jednej lub kilku aktualizacji:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Aktualizacje oprogramowania**.
   Zostanie wyświetlona lista dostępnych aktualizacji.
2. Wybierz uaktualnienia, które chcesz zatwierdzić lub odrzucić.
3. Kliknij **Zatwierdź**, aby zatwierdzić wybrane aktualizacje, lub **Odrzuć**, aby odrzucić wybrane aktualizacje.
   Domyślna wartość to *Niezdefiniowane*.

Wybrane aktualizacje posiadają stany, które zdefiniowałeś.

Istnieje również możliwość zmiany stanu zatwierdzenia we właściwościach określonej aktualizacji.

W celu zatwierdzenia lub odrzucenia aktualizacji w jej właściwościach:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Aktualizacje oprogramowania**.
   Zostanie wyświetlona lista dostępnych aktualizacji.
2. Kliknij nazwę aktualizacji, którą chcesz zatwierdzić lub odrzucić.
   Zostanie otwarte okno właściwości aktualizacji.
3. W sekcji **Ogólne** wybierz stan dla aktualizacji, zmieniając opcję **Stan zatwierdzenia aktualizacji**. Możesz wybrać stan *Zatwierdzono*, *Odrzucono* lub *Nie zdefiniowano*.
4. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Wybrana aktualizacja posiada stan, który zdefiniowałeś.

Jeśli ustawisz stan **Odrzucono** dla aktualizacji oprogramowania firm trzecich, te aktualizacje nie zostaną zainstalowane na urządzeniach, dla których planowane było ich zainstalowanie, ale jeszcze nie zostały zainstalowane. Uaktualnienia pozostaną na urządzeniach, na których zostały już zainstalowane. Jeśli musisz je usunąć, możesz je usunąć ręcznie lokalnie.

Tworzenie zadania Wykonaj synchronizację Windows Update

Zadanie *Wykonaj synchronizację Windows Update* jest dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Zadanie *Wykonaj synchronizację Windows Update* jest wymagane, jeśli chcesz używać serwera administracyjnego jako serwera WSUS. W tym przypadku serwer administracyjny pobiera aktualizacje Windows do bazy danych i dostarcza aktualizacje Windows Update na urządzeniach klienckich w trybie scentralizowanym za pośrednictwem Agentów sieciowych. Jeśli sieć nie wykorzystuje serwera WSUS, każde urządzenie klienckie pobiera aktualizacje Microsoft niezależnie z zewnętrznych serwerów.

Zadanie *Wykonaj synchronizację Windows Update* pobiera tylko metadane z serwerów Microsoft. Kaspersky Security Center pobiera aktualizacje po uruchomieniu zadania instalacji aktualizacji i tylko te aktualizacje, które wybrałeś do instalacji.

Podczas wykonywania zadania **Wykonaj synchronizację Windows Update** aplikacja pobiera listę bieżących aktualizacji z serwera aktualizacji Microsoft. Następnie, Kaspersky Security Center tworzy listę aktualizacji, które są przestarzałe. Przy kolejnym uruchomieniu zadania **Wyszukiwanie luk i wymaganych aktualizacji** program Kaspersky Security Center oznaczy wszystkie przestarzałe aktualizacje i ustawi dla nich czas usunięcia. Przy kolejnym uruchomieniu zadania **Wykonaj synchronizację Windows Update** wszystkie aktualizacje, które zostały oznaczone do usunięcia 30 dni wcześniej, zostaną usunięte. Kaspersky Security Center sprawdza także obecność przestarzałych aktualizacji, które zostały oznaczone do usunięcia ponad 180 dni temu, a następnie usuwa te starsze aktualizacje.

Jeśli zadanie **Wykonaj synchronizację Windows Update** zostanie zakończone, a przestarzałe aktualizacje zostaną usunięte, baza danych może wciąż posiadać kody skrótów odnoszące się do plików usuniętych aktualizacji, a także odpowiednie pliki w plikach %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (jeśli zostały pobrane wcześniej). Możesz uruchomić zadanie **Konserwacja Serwera administracyjnego**, aby usunąć te przestarzałe wpisy z bazy danych oraz odpowiednie pliki.

W celu utworzenia zadania Wykonaj synchronizację Windows Update:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Wykonaj synchronizację Windows Update**.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Włącz opcję **Pobierz ekspresowe pliki instalacyjne** jeśli chcesz, aby pliki ekspresowej aktualizacji były pobierane podczas uruchamiania zadania.

   Jeśli Kaspersky Security Center synchronizuje aktualizacje z Microsoft Windows Update Servers, informacje o wszystkich plikach są zapisywane w bazie danych Serwera administracyjnego. Wszystkie pliki niezbędne dla aktualizacji zostają także pobrane na dysk podczas interakcji z Windows Update Agent. Kaspersky Security Center zapisuje informacje o plikach aktualizacji ekspresowej w bazie danych i pobiera je, gdy jest to konieczne. Pobranie plików aktualizacji ekspresowej prowadzi do zmniejszenia wolnego miejsca na dysku.

   Aby uniknąć zmniejszenia ilości wolnego miejsca na dysku oraz zmniejszyć ruch sieciowy, wyłącz opcję **Pobierz ekspresowe pliki instalacyjne**.
6. Wybierz aplikacje, dla których chcesz pobrać aktualizacje.

   Jeśli pole **Wszystkie aplikacje** jest zaznaczone, uaktualnienia będą pobierane dla wszystkich istniejących aplikacji, a także dla wszystkich aplikacji, które mogą zostać wydane w przyszłości.
7. Wybierz kategorie aktualizacji, które chcesz pobrać na serwer administracyjny.

   Jeśli pole **Wszystkie kategorie** jest zaznaczone, uaktualnienia będą pobierane dla wszystkich istniejących kategorii uaktualnień, a także dla wszystkich kategorii, które mogą pojawić się w przyszłości.
8. Wybierz języki lokalizacji aktualizacji, które chcesz pobrać na Serwer administracyjny. Wybierz jedną z następujących opcji:

   - **Pobierz wszystkie języki, wraz z nowymi**

     Jeśli ta opcja jest zaznaczona, na Serwer administracyjny zostaną pobrane wszystkie wersje językowe aktualizacji. Domyślnie opcja ta jest zaznaczona.

   - **Pobierz wybrane języki**

Jeśli ta opcja jest zaznaczona, z listy wersji językowych możesz wybrać te, które powinny zostać pobrane na Serwer administracyjny.

9. Określ, które konto ma być używane podczas uruchamiania zadania. Wybierz jedną z następujących opcji:

   - **Konto domyślne**

     Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

     Domyślnie opcja ta jest zaznaczona.

   - **Określ konto**

     Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

10. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

11. Kliknij przycisk **Zakończ**.

    Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

12. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

13. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

14. Kliknij przycisk **Zapisz**.

Zadanie zostało utworzone i skonfigurowane.

Automatyczne aktualizowanie aplikacji innych firm

Niektóre aplikacje innych firm mogą być aktualizowane automatycznie. Producent aplikacji definiuje, czy aplikacja obsługuje funkcję automatycznej aktualizacji. Jeśli aplikacja innej firmy, zainstalowana na zarządzanym urządzeniu, obsługuje automatyczną aktualizację, możesz określić ustawienie automatycznej aktualizacji we właściwościach aplikacji. Po zmianie ustawienia automatycznej aktualizacji Agenty sieciowe stosują nowe ustawienie na każdym zarządzanym urządzeniu, na którym jest zainstalowana aplikacja.

Ustawienie automatycznej aktualizacji jest niezależne od innych obiektów i ustawień funkcji Zarządzanie lukami i poprawkami. Na przykład, to ustawienie nie zależy od stanu zatwierdzenia aktualizacji ani od zadań instalacji aktualizacji, takich jak *Zainstaluj wymagane aktualizacje i napraw luki*, *Zainstaluj aktualizacje Windows* oraz *Napraw luki*.

W celu skonfigurowania ustawienia automatycznej aktualizacji dla aplikacji innej firmy:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Rejestr aplikacji**.

2. Kliknij nazwę aplikacji, dla której chcesz zmienić ustawienie automatycznej aktualizacji.

   Aby uprościć wyszukiwanie, możesz przefiltrować listę według kolumny **Stan aktualizacji automatycznych**.

Zostanie otwarte okno właściwości aplikacji.

3. W sekcji **Ogólne** wybierz wartość dla następującego ustawienia:

   Stan aktualizacji automatycznych

   Wybierz jedną z następujących opcji:

   - **Nie zdefiniowano**

     Funkcja automatycznej aktualizacji jest wyłączona. Kaspersky Security Center instaluje aktualizacje aplikacji innej firmy, korzystając z zadań: *Zainstaluj wymagane aktualizacje i napraw luki*, *Zainstaluj aktualizacje Windows* i *Napraw luki*.

   - **Dozwolony**

     Jak tylko wydawca opublikuje aktualizację dla aplikacji, ta aktualizacja jest automatycznie instalowana na zarządzanych urządzeniach. Dodatkowe działania nie są wymagane.

   - **Zablokowano**

     Aktualizacje aplikacji nie są instalowane automatycznie. Kaspersky Security Center instaluje aktualizacje aplikacji innej firmy, korzystając z zadań: *Zainstaluj wymagane aktualizacje i napraw luki*, *Zainstaluj aktualizacje Windows* i *Napraw luki*.

4. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Ustawienie automatycznej aktualizacji jest stosowane do wybranej aplikacji.

Eliminowanie luk w oprogramowaniu innych firm

Ta sekcja opisuje funkcje Kaspersky Security Center, które dotyczą eliminowania luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach.

Scenariusz: Wyszukiwanie i usuwanie luk w oprogramowaniu firm trzecich

Ta sekcja zawiera scenariusz wyszukiwania i naprawiania luk na zarządzanych urządzeniach działających pod kontrolą systemu Windows. Możesz znaleźć i naprawić luki w oprogramowaniu w systemie operacyjnym oraz w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft.

Wymagania wstępne

- Kaspersky Security Center zostanie wdrożony w Twojej organizacji.
- W Twojej organizacji znajdują się zarządzane urządzenia działające pod kontrolą systemu Windows.
- Połączenie internetowe w przypadku Serwera administracyjnego jest wymagane, aby można było wykonywać następujące zadania:
  - Sporządzanie listy zalecanych poprawek dla luk w oprogramowaniu firmy Microsoft. Lista jest tworzona i regularnie aktualizowana przez specjalistów z Kaspersky.

- Naprawianie luk w oprogramowaniu firm trzecich innym niż oprogramowanie firmy Microsoft.

Etapy

Wyszukiwanie i naprawianie luk w oprogramowaniu odbywa się w etapach:

1. **Skanowanie luk w oprogramowaniu zainstalowanym na zarządzanych urządzeniach**

   Aby odszukać luki w oprogramowaniu zainstalowanym na zarządzanych urządzeniach, uruchom zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Jeśli to zadanie zostanie zakończone, Kaspersky Security Center pobierze listy wykrytych luk i żądanych aktualizacji dla oprogramowania firm trzecich zainstalowanego na urządzeniach, które określiłeś we właściwościach zadania.

   Zadanie *Wyszukiwanie luk i wymaganych aktualizacji* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Jeśli nie uruchamiałeś kreatora, uruchom go teraz lub utwórz zadanie ręcznie.

   Dostępne instrukcje:

   - Konsola administracyjna: Skanowanie aplikacji w poszukiwaniu luk, Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji
   - Kaspersky Security Center Web Console: Tworzenie zadania Wyszukiwanie luk i wymaganych aktualizacji, Ustawienia zadania Wyszukiwanie luk i wymaganych aktualizacji

2. **Analizowanie listy wykrytych luk w oprogramowaniu**

   Przejrzyj listę **Luki w oprogramowaniu** i zdecyduj, które luki mają zostać naprawione. Aby przejrzeć szczegółowe informacje o każdej luce, kliknij nazwę luki na liście. Dla każdej luki na liście możesz także przejrzeć statystyki dotyczące luki na zarządzanych urządzeniach.

   Dostępne instrukcje:

   - Konsola administracyjna: Przeglądanie informacji o lukach w oprogramowaniu, Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach
   - Kaspersky Security Center Web Console: Przeglądanie informacji o lukach w oprogramowaniu, Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

3. **Konfigurowanie naprawy luk**

   Jeśli luki w oprogramowaniu zostaną wykryte, możesz naprawić luki w oprogramowaniu na zarządzanych urządzeniach, korzystając z zadania *Zainstaluj wymagane aktualizacje i napraw luki* lub zadania *Napraw luki*.

   Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft, zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawę kilku luk zgodnie z pewnymi regułami. Pamiętaj, że to zadanie może zostać utworzone tylko wtedy, gdy masz licencję dla funkcji Zarządzanie lukami i poprawkami. Aby naprawić luki w oprogramowaniu, zadanie *Zainstaluj wymagane aktualizacje i napraw luki* używa zalecanych aktualizacji oprogramowania.

   Zadanie *Napraw luki* nie wymaga opcji licencjonowania dla funkcji Zarządzanie lukami i poprawkami. Aby użyć tego zadania, należy ręcznie określić poprawki użytkownika dla luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla programów innych firm.

   Możesz uruchomić Kreator naprawiania luk, który tworzy jedno z tych zadań automatycznie, lub możesz utworzyć jedno z tych zadań ręcznie.

   Dostępne instrukcje:

   - Konsola administracyjna: Wybieranie poprawek użytkownika dla luk w programach innych firm, Naprawianie luk w aplikacjach

- Kaspersky Security Center Web Console: Wybieranie poprawek użytkownika dla luk w programach innych firm, Naprawianie luk w programach innych firm, Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki

4. **Konfigurowanie terminarza zadań**

   Aby upewnić się, że lista luk jest zawsze aktualna, skonfiguruj zadanie *Wyszukiwanie luk i wymaganych aktualizacji* tak, aby było uruchamiane automatycznie od czasu do czasu. Zalecana przeciętna częstotliwość uruchamiania to raz na tydzień.

   Jeśli utworzyłeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, możesz skonfigurować terminarz tak, aby zadanie było uruchamiane z tą samą częstotliwością co zadanie *Wyszukiwanie luk i wymaganych aktualizacji* lub rzadziej. Podczas ustawiania terminarza zadania *Napraw luki* należy pamiętać, żeby wybrać poprawki dla oprogramowania Microsoft lub określić poprawki użytkownika dla oprogramowania innych firm za każdym razem przed rozpoczęciem zadania.

   Jeśli konfigurujesz terminarz uruchamiania zadania, upewnij się, że zadanie naprawy luki zostanie uruchomione po zakończeniu zadania *Wyszukiwanie luk i wymaganych aktualizacji*.

5. **Ignorowanie luk w oprogramowaniu (opcjonalne)**

   Jeśli chcesz, możesz zignorować luki w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

   Dostępne instrukcje:

   - Konsola administracyjna: Ignorowanie luk w oprogramowaniu
   - Kaspersky Security Center Web Console: Ignorowanie luk w oprogramowaniu

6. **Uruchamianie zadania naprawy luk**

   Uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Napraw lukę*. Po zakończeniu zadania, upewnij się, że na liście zadań posiada stan *Zakończone pomyślnie*.

7. **Utwórz raport dotyczący wyników naprawy luk w oprogramowaniu (opcjonalne)**

   Aby wyświetlić szczegółowe statystyki dotyczące naprawy luk, wygeneruj Raport o lukach. Raport wyświetla informacje o lukach w oprogramowaniu, które nie zostały naprawione. Dzięki temu możesz wiedzieć o wyszukiwaniu i naprawie luk w programach innych firm, w tym w oprogramowaniu firmy Microsoft, w swojej organizacji.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie i przeglądanie raportu
   - Kaspersky Security Center Web Console: Tworzenie i przeglądanie raportu

8. **Sprawdzanie konfiguracji wyszukiwania i naprawy luk w programach innych firm**

   Upewnij się, że wykonałeś następujące czynności:

   - Uzyskałeś i przejrzałeś listę luk w oprogramowaniu na zarządzanych urządzeniach
   - Zignorowałeś luki w oprogramowaniu, jeśli chciałeś
   - Skonfigurowałeś zadanie naprawy luk
   - Skonfigurowałeś terminarz zadań wyszukiwania i naprawy luk w oprogramowaniu, aby były uruchamianie po kolei
   - Sprawdziłeś, czy zadanie naprawy luk w oprogramowaniu zostało uruchomione

Wyniki

Jeśli utworzyłeś i skonfigurowałeś zadanie *Zainstaluj wymagane aktualizacje i napraw luki*, luki zostają naprawione na zarządzanych urządzeniach automatycznie. Jeśli zadanie zostaje uruchomione, zestawia listę dostępnych aktualizacji oprogramowania z regułami określonymi w ustawieniach zadania. Wszystkie aktualizacje oprogramowania, które spełniają kryteria w regułach, zostaną pobrane do repozytorium Serwera administracyjnego i zostaną zainstalowane w celu naprawy luk w oprogramowaniu.

Jeśli utworzyłeś zadanie *Napraw luki*, naprawione zostaną tylko luki w oprogramowaniu firmy Microsoft.

Informacje o wyszukiwaniu i eliminowaniu luk w oprogramowaniu

Kaspersky Security Center wykrywa i naprawia luki w oprogramowaniu na zarządzanych urządzeniach działających pod kontrolą systemów operacyjnych z rodziny Microsoft Windows. Luki są wykrywane w systemie operacyjnym i w oprogramowaniu innych firm, w tym w oprogramowaniu firmy Microsoft.

Wyszukiwanie luk w oprogramowaniu

Aby znaleźć luki w oprogramowaniu, Kaspersky Security Center wykorzystuje znaki charakterystyczne z bazy danych znanych zagrożeń. Ta baza danych jest tworzona przez specjalistów z Kaspersky. Zawiera informacje o lukach, takie jak opis luki, data wykrycia luki, priorytet luki. Szczegóły dotyczące luk w oprogramowaniu można znaleźć na stronie internetowej Kaspersky.

Kaspersky Security Center wykorzystuje zadanie *Wyszukiwanie luk i wymaganych aktualizacji* do wykrywania luk w oprogramowaniu.

Naprawianie luk w oprogramowaniu

Aby naprawić luki w oprogramowaniu, Kaspersky Security Center używa aktualizacji oprogramowania opublikowanych przez producentów oprogramowania. Metadane aktualizacji oprogramowania są pobierane z repozytorium Serwera administracyjnego w wyniku uruchomienia następującego zadania:

- *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. To zadanie jest przeznaczone do pobrania metadanych aktualizacji dla Kaspersky i oprogramowania firm trzecich. To zadanie jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center. Możesz ręcznie utworzyć zadanie Pobierz uaktualnienia do repozytorium Serwera administracyjnego.

- *Wykonaj synchronizację Windows Update*. To zadanie jest przeznaczone do pobrania metadanych aktualizacji dla oprogramowania firmy Microsoft.

Aktualizacje oprogramowania eliminujące luki mogą być w postaci pełnych pakietów dystrybucyjnych lub poprawek. Aktualizacje oprogramowania, które eliminują luki w oprogramowaniu, nazywane są *poprawkami*. *Zalecane poprawki* to takie poprawki, które są zalecane do zainstalowania przez specjalistów z Kaspersky. *Poprawki użytkownika* to takie poprawki, które są ręcznie określane do zainstalowania przez użytkowników. Aby zainstalować poprawkę użytkownika, należy utworzyć pakiet instalacyjny zawierający tę poprawkę.

Jeśli posiadasz licencję dla Kaspersky Security Center z funkcją Zarządzanie lukami i poprawkami, aby usunąć luki w oprogramowaniu, możesz użyć zadania *Zainstaluj wymagane aktualizacje i napraw luki*. To zadanie automatycznie eliminuje kilka luk poprzez zainstalowanie zalecanych poprawek. Dla tego zadania można ręcznie skonfigurować pewne reguły do naprawy kilku luk.

Jeśli nie posiadasz licencji dla Kaspersky Security Center z funkcją Zarządzanie lukami i poprawkami, aby usunąć luki w oprogramowaniu, możesz użyć zadania *Napraw luki*. Korzystając z tego zadania, możesz wyeliminować luki poprzez zainstalowanie zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm.

Ze względów bezpieczeństwa wszelkie aktualizacje oprogramowania innych firm, które instalujesz za pomocą funkcji Zarządzanie lukami i poprawkami, są automatycznie skanowane w poszukiwaniu złośliwego oprogramowania przez technologie firmy Kaspersky. Technologie te są używane do automatycznego sprawdzania plików i obejmują skanowanie antywirusowe, analizę statyczną, analizę dynamiczną, analizę zachowania w środowisku sandbox i uczenie maszynowe.

Eksperci firmy Kaspersky nie przeprowadzają ręcznej analizy aktualizacji oprogramowania innych firm, które są instalowane przez funkcję Zarządzanie lukami i poprawkami. Ponadto eksperci z firmy Kaspersky nie wyszukują luk w zabezpieczeniach (znanych lub nieznanych) ani nieudokumentowanych funkcji w takich aktualizacjach, a także nie przeprowadzają innych rodzajów analizy aktualizacji innych, niż określone w powyższym akapicie.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Aby naprawić niektóre luki w oprogramowaniu, należy zaakceptować Umowę licencyjną (EULA) dla instalowanego oprogramowania, jeśli wymagane jest zaakceptowanie Umowy licencyjnej. Jeśli odrzucisz Umowę licencyjną, luka w oprogramowaniu nie zostanie wyeliminowana.

Eliminowanie luk w oprogramowaniu innych firm

Po uzyskaniu listy luk w oprogramowaniu możliwe jest wyeliminowanie luk w oprogramowaniu na zarządzanych urządzeniach działających pod kontrolą systemu Windows. Luki w oprogramowaniu w systemie operacyjnym i oprogramowaniu innych firm, w tym w oprogramowaniu firmy Microsoft, można naprawić, tworząc i uruchamiając zadanie *Napraw luki* lub zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

Opcjonalnie możesz utworzyć zadanie naprawiania luk w oprogramowaniu w następujący sposób:

- Otwierając listę luk i określając, które luki należy naprawić.

  W rezultacie powstaje nowe zadanie naprawy luk w oprogramowaniu. Istnieje możliwość dodania wybranych luk do istniejącego zadania.

- Uruchamiając Kreator naprawiania luk.

  Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

  Kreator upraszcza tworzenie i konfigurację zadania naprawy luki w zabezpieczeniach i pozwala wyeliminować tworzenie zbędnych zadań zawierających te same aktualizacje do zainstalowania.

Naprawianie luk w oprogramowaniu przy użyciu listy luk w zabezpieczeniach

W celu wyeliminowania luk w oprogramowaniu:

1. Otwórz jedną z list luk:

   - Aby otworzyć ogólną listę luk, w menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.
   - Aby otworzyć listę luk dla zarządzanego urządzenia, w menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia** → <device name> → **Zaawansowane** → **Luki w oprogramowaniu**.
   - Aby otworzyć listę luk dla określonej aplikacji, w menu głównym przejdź do **Operacje** → **Aplikacje innych firm** → **Rejestr aplikacji** → <application name> → **Luki**.

   Zostanie wyświetlona lista luk w oprogramowaniu innych firm.

2. Wybierz jedną lub więcej luk na liście, a następnie kliknij przycisk **Napraw lukę**.

   Jeśli brakuje zalecanej aktualizacji oprogramowania do naprawy jednej z wybranych luk, zostanie wyświetlony odpowiedni komunikat.

   Aby naprawić niektóre luki w oprogramowaniu, należy zaakceptować Umowę licencyjną dla instalowanego oprogramowania (EULA), jeśli wymagane jest zaakceptowanie Umowy licencyjnej. Jeśli odrzucisz Umowę licencyjną, luka w oprogramowaniu nie zostanie wyeliminowana.

3. Wybierz jedną z następujących opcji:

   - **Nowe zadanie**

     Zostanie uruchomiony Kreator tworzenia nowego zadania. Jeśli masz licencję Zarządzania lukami i poprawkami, domyślnie wybrany jest typ zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Jeśli nie masz licencji, domyślnie wybrany jest typ zadania *Napraw luki*. Aby zakończyć tworzenie zadania, postępuj zgodnie z instrukcjami kreatora.

   - **Napraw lukę (dodaj regułę do określonego zadania)**

     Wybierz zadanie, do którego chcesz dodać wybrane luki. Jeśli masz licencję Zarządzania lukami i poprawkami, wybierz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*. Nowa reguła eliminacji wybranych luk zostanie automatycznie dodania do wybranego zadania. Jeśli nie masz licencji, wybierz zadanie *Napraw luki*. Wybrane luki zostaną dodane do właściwości zadania.

     Zostanie otwarte okno właściwości zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

   Jeśli wybrałeś utworzenie nowego zadania, zadanie zostanie utworzone i wyświetlone na liście zadań, w sekcji **Urządzenia** → **Zadania**. Jeśli wybrałeś dodanie luk do istniejącego zadania, luki zostaną zapisane we właściwościach zadania.

Aby wyeliminować luki w oprogramowaniu firm trzecich, uruchom zadanie *Zainstaluj wymagane aktualizacje i napraw luki* lub zadanie *Napraw luki*. Jeśli utworzyłeś zadanie *Napraw luki*, powinieneś ręcznie określić aktualizacje oprogramowania w celu naprawy luk w oprogramowaniu, wymienionych w ustawieniach zadania.

Naprawianie luk w oprogramowaniu przy użyciu kreatora naprawiania luk

Funkcje kreatora naprawiania luk są dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Aby naprawić luki w oprogramowaniu przy użyciu kreatora naprawiania luk:

1. W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

Zostanie wyświetlona lista luk w oprogramowaniu innych firm, zainstalowanym na zarządzanych urządzeniach.

2. Zaznacz pole obok luki, który chcesz wyeliminować.

3. Kliknij przycisk **Uruchom kreatora naprawiania luk**.

   Zostanie uruchomiony Kreator naprawiania luk. Strona **Wybierz zadanie naprawiania luk** wyświetla listę wszystkich istniejących zadań następujących typów:

   - *Zainstaluj wymagane aktualizacje i napraw luki*
   - *Zainstaluj aktualizacje Windows*
   - *Napraw luki*

   Nie można zmodyfikować ostatnich dwóch typów zadań, aby zainstalować nowe aktualizacje. Aby zainstalować nowe aktualizacje, możesz użyć tylko zadania *Zainstaluj wymagane aktualizacje i napraw luki*.

4. Jeśli chcesz, aby kreator wyświetlał tylko te zadania, które usuwają wybraną lukę, włącz opcję **Pokaż tylko zadania naprawiające tę lukę**.

5. Wybierz, co chcesz zrobić:

   - Aby rozpocząć zadanie, zaznacz pole wyboru obok nazwy zadania, a następnie kliknij przycisk **Uruchom**.
   - Aby dodać nową regułę do istniejącego zadania:

     a. Zaznacz pole obok nazwy zadania i kliknij przycisk **Dodaj regułę**.

     b. Na wyświetlonej stronie skonfiguruj nową regułę:

     - Reguła dla naprawiania luk tego priorytetu

       Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

       Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

       Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

       Domyślnie opcja ta jest wyłączona.

     - **Reguła naprawiania luk za pomocą aktualizacji tego samego typu, co aktualizacja zdefiniowana jako zalecana dla wybranej luki** (dostępna tylko dla luk w oprogramowaniu Microsoft)
     - **Reguła naprawiania luk w aplikacjach według wybranego dostawcy** (dostępne tylko dla luk w oprogramowaniu innych firm)
     - **Reguła naprawiania luk we wszystkich wersjach wybranej aplikacji** (dostępne tylko dla luk w oprogramowaniu innych firm)
     - **Reguła naprawiania wybranej luki**
     - Akceptuj aktualizacje, które naprawiają tę lukę

Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

Domyślnie opcja ta jest wyłączona.

c. Kliknij przycisk **Dodaj**.

- W celu utworzenia zadania:

a. Kliknij przycisk **Nowe zadanie**.

b. Na wyświetlonej stronie skonfiguruj nową regułę:

- Reguła dla naprawiania luk tego priorytetu

Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż priorytet wybranej aktualizacji (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

Domyślnie opcja ta jest wyłączona.

- **Reguła naprawiania luk za pomocą aktualizacji tego samego typu, co aktualizacja zdefiniowana jako zalecana dla wybranej luki** (dostępna tylko dla luk w oprogramowaniu Microsoft)
- **Reguła naprawiania luk w aplikacjach według wybranego dostawcy** (dostępne tylko dla luk w oprogramowaniu innych firm)
- **Reguła naprawiania luk we wszystkich wersjach wybranej aplikacji** (dostępne tylko dla luk w oprogramowaniu innych firm)
- **Reguła naprawiania wybranej luki**
- Akceptuj aktualizacje, które naprawiają tę lukę

Instalacja wybranej aktualizacji zostanie zatwierdzona. Włącz tę opcję, jeśli niektóre stosowane reguły instalacji aktualizacji zezwalają tylko na instalację zaakceptowanych aktualizacji.

Domyślnie opcja ta jest wyłączona.

c. Kliknij przycisk **Dodaj**.

Jeśli wybrano rozpoczęcie zadania, możesz zamknąć kreatora. Zadanie zakończy się w tle. Dalsze działania nie są wymagane.

Jeśli wybrałeś dodanie reguły do istniejącego zadania, zostanie otwarte okno właściwości zadania. Nowa reguła została już dodana do właściwości zadania. Możesz przejrzeć lub zmodyfikować regułę lub ustawienia innego zadania. Kliknij przycisk **Zapisz**, aby zapisać zmiany.

Jeśli chcesz utworzyć zadanie, kontynuuj tworzenie zadania w kreatorze tworzenia nowego zadania. Nowa reguła dodana w kreatorze naprawiania luk zostanie wyświetlona w kreatorze tworzenia nowego zadania. Po zakończeniu pracy kreatora, do listy zadań zostanie dodane zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.

Tworzenie zadania Napraw luki

Zadanie *Napraw luki* pozwala naprawić luki w oprogramowaniu na zarządzanych urządzeniach z systemem Windows. Możesz naprawić luki w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft.

Jeśli nie masz licencji Zarządzania lukami i poprawkami, nie możesz tworzyć nowych zadań typu *Napraw luki*. Aby naprawić nowe luki, możesz dodać je do istniejącego zadania *Napraw luki*. Zalecamy użycie zadania *Zainstaluj wymagane aktualizacje i napraw luki* zamiast zadania *Napraw luki*. Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* umożliwia automatyczne instalowanie wielu aktualizacji i naprawianie wielu luk w zabezpieczeniach, zgodnie z określonymi przez Ciebie regułami.

Interakcja użytkownika może być wymagana podczas aktualizacji aplikacji innej firmy lub naprawy luki w aplikacji innej firmy na zarządzanym urządzeniu. Na przykład, użytkownik może zostać poproszony o zamknięcie aplikacji innej firmy, jeśli jest ona aktualnie otwarta.

W celu utworzenia zadania Napraw luki:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Napraw luki**.
4. Określ nazwę tworzonego zadania.

   Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("* <>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Kliknij przycisk **Dodaj**.

   Zostanie otwarta lista luk.
7. Wybierz luki, które chcesz naprawić, a następnie kliknij **OK**.

   Luki w oprogramowaniu firmy Microsoft zwykle zawierają zalecane poprawki. Nie są wymagane żadne dodatkowe czynności. W przypadku luk w zabezpieczeniach oprogramowania innych producentów należy najpierw określić poprawkę użytkownika dla każdej luki, którą chcesz naprawić. Następnie będzie można dodać te luki do zadania *Napraw luki*.
8. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

   - **Nie uruchamiaj ponownie urządzenia**

Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

  Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

  Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

  Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- **Uruchom ponownie po (min)**

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- **Wymuś zamknięcie aplikacji dla zablokowanych sesji**

Uruchomione aplikacje mogą uniemożliwić ponowne uruchomienie urządzenia klienckiego. Na przykład, jeśli dokument jest edytowany w edytorze tekstu i nie zostanie zapisany.

Jeśli ta opcja jest włączona, zostaje wymuszone zamknięcie takich aplikacji na zablokowanym urządzeniu przed jego ponownym uruchomieniem. W wyniku tego działania użytkownicy mogą utracić niezapisane zmiany.

Jeśli ta opcja jest wyłączona, zablokowane urządzenie nie zostanie uruchomione ponownie. Stan zadania na tym urządzeniu informuje, że wymagane jest ponowne uruchomienie urządzenia. Użytkownicy muszą ręcznie zamknąć wszystkie aplikacje uruchomione na zablokowanych urządzeniach i uruchomić ponownie te urządzenia.

Domyślnie opcja ta jest wyłączona.

9. Określ ustawienia konta:

- **Konto domyślne**

  Zadanie zostanie uruchomione z poziomu tego samego konta co aplikacja, która wykonuje to zadanie.

  Domyślnie opcja ta jest zaznaczona.

- **Określ konto**

  Uzupełnij pola **Konto** i **Hasło**, aby określić szczegóły konta, z poziomu którego uruchamiane jest zadanie. Konto musi posiadać wystarczające uprawnienia dla tego zadania.

- **Konto**

  Konto, z poziomu którego zadanie jest uruchamiane.

- **Hasło**

  Hasło do konta, z poziomu którego zadanie będzie uruchamiane.

10. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

11. Kliknij przycisk **Zakończ**.

    Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

12. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

13. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

14. Kliknij przycisk **Zapisz**.

Zadanie zostało utworzone i skonfigurowane.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest dostępne tylko dla licencji Zarządzanie lukami i poprawkami.

Zadanie *Zainstaluj wymagane aktualizacje i napraw luki* jest używane do aktualizacji i naprawy luk w oprogramowaniu firm trzecich, w tym w oprogramowaniu firmy Microsoft, zainstalowanym na zarządzanych urządzeniach. To zadanie umożliwia zainstalowanie kilku aktualizacji i naprawę kilku luk zgodnie z pewnymi regułami.

W celu zainstalowania aktualizacji lub wyeliminowania luk za pomocą zadania *Zainstaluj wymagane aktualizacje i napraw luki*, możesz wykonać jedną z następujących czynności:

- Uruchom kreator instalacji aktualizacji lub Kreator naprawiania luk.
- Utwórz zadanie *Zainstaluj wymagane aktualizacje i napraw luki*.
- Dodaj regułę instalacji aktualizacji do istniejącego pliku *Zainstaluj wymagane aktualizacje i napraw luki* zadanie.

Tworzenie zadania Zainstaluj wymagane aktualizacje i napraw luki:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.
3. Dla aplikacji Kaspersky Security Center wybierz typ zadania **Zainstaluj wymagane aktualizacje i napraw luki**.

   Jeśli zadanie nie jest wyświetlane, sprawdź, czy Twoje konto ma uprawnienia **Odczyt**, **Modyfikuj** i **Wykonaj** dla obszaru funkcjonalnego **Zarządzanie systemem: Zarządzanie lukami w zabezpieczeniach i poprawkami**. Bez tych praw dostępu nie można utworzyć ani skonfigurować zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
4. Określ nazwę tworzonego zadania. Nazwa zadania nie może zawierać więcej niż 100 znaków oraz nie może zawierać żadnych znaków specjalnych ("*<>?\:|).
5. Wybierz urządzenia, do których zadanie zostanie przypisane.
6. Określ zasady instalacji aktualizacji, a następnie określ następujące ustawienia:

   - **Uruchom instalację podczas ponownego uruchamiania lub wyłączania urządzenia**

     Jeśli ta opcja jest włączona, aktualizacje są instalowane po ponownym uruchomieniu lub zamknięciu urządzenia. W innym przypadku aktualizacje są instalowane zgodnie z terminarzem.

     Użyj tej opcji, jeśli instalowanie aktualizacji może wpłynąć na działanie urządzenia.

     Domyślnie opcja ta jest wyłączona.

   - **Zainstaluj wymagane ogólne składniki systemu**

Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

Domyślnie opcja ta jest wyłączona.

- **Zezwól na instalację nowych wersji aplikacji podczas aktualizacji**

  Jeśli ta opcja jest włączona, aktualizacje są dozwolone, gdy powodują zainstalowanie nowej wersji aplikacji.

  Jeśli ta opcja jest wyłączona, aplikacja nie zostanie zaktualizowana. W takiej sytuacji możesz ręcznie zainstalować nowe wersje aplikacji lub użyć w tym celu innego zadania. Na przykład, możesz użyć tej opcji, jeśli struktura Twojej firmy nie jest obsługiwana przez nową wersję aplikacji lub jeśli chcesz sprawdzić aktualizację w infrastrukturze testowej.

  Domyślnie opcja ta jest włączona.

  > Aktualizowanie aplikacji może spowodować problemy z działaniem powiązanych aplikacji zainstalowanych na urządzeniach klienckich.

- **Pobierz aktualizacje na urządzenie, ale ich nie instaluj**

  Jeśli ta opcja jest włączona, aplikacja pobierze uaktualnienia na urządzenie, ale nie zainstaluje ich automatycznie. Możesz ręcznie zainstalować pobrane aktualizacje.

  Aktualizacje Microsoft są pobierane do folderu systemowego Windows. Aktualizacje aplikacji firm trzecich (aplikacje innych producentów niż Kaspersky i Microsoft) są pobierane do folderu określonego w polu **Folder do pobierania aktualizacji**.

  Jeśli ta opcja jest wyłączona, aktualizacje są instalowane na urządzeniu automatycznie.

  Domyślnie opcja ta jest wyłączona.

- **Folder do pobierania aktualizacji**

  Ten folder jest używany do pobierania aktualizacji aplikacji innych firm (aplikacji innych producentów niż Kaspersky i Microsoft).

- **Włącz diagnostykę zaawansowaną**

Jeśli ta funkcja jest włączona, Agent sieciowy zapisuje pliki śledzenia nawet wtedy, gdy śledzenie jest wyłączone dla Agenta sieciowego w Narzędziu zdalnej diagnostyki Kaspersky Security Center. Śledzenie jest zapisywane do dwóch plików; całkowity rozmiar obu plików jest określany przez wartość **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**. Jeśli oba pliki są pełne, Agent sieciowy ponownie uruchamia zapisywanie do tych plików. Pliki zawierające ślady są przechowywane w folderze %WINDIR%\Temp. Te pliki są dostępne w narzędziu do zdalnej diagnostyki - możesz je pobrać lub usunąć.

Jeśli ta funkcja jest wyłączona, Agent sieciowy zapisuje śledzenie zgodnie z ustawieniami Narzędzia zdalnej diagnostyki Kaspersky Security Center. Nie są zapisywane żadne dodatkowe pliki śledzenia.

Jeśli tworzysz zadanie, nie musisz włączać zaawansowanej diagnostyki. Tej funkcji można użyć później, jeśli, na przykład, uruchomienie zadania nie powiedzie się na niektórych urządzeniach i chcesz uzyskać dodatkowe informacje podczas uruchamiania innego zadania.

Domyślnie opcja ta jest wyłączona.

- **Maksymalny rozmiar plików zaawansowanej diagnostyki, w MB**

  Domyślna wartość to 100 MB, a dostępne wartości mieszczą się między 1 MB a 2048 MB. Specjalista z pomocy technicznej Kaspersky może poprosić o zmianę domyślnej wartości, jeśli informacje w plikach zaawansowanej diagnostyki, które wysłałeś, nie są wystarczające do rozwiązania problemu.

7. Określ ustawienia ponownego uruchamiania systemu operacyjnego:

- **Nie uruchamiaj ponownie urządzenia**

  Urządzenia klienckie nie są automatycznie uruchamiane ponownie po działaniu. Aby zakończyć działanie, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**

  Urządzenia klienckie są zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia działania. Opcja jest przydatna, gdy zadania są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**

  Na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Ta opcja jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia.

  Domyślnie opcja ta jest zaznaczona.

- **Ponawiaj pytanie co (min)**

Jeśli ta opcja jest włączona, aplikacja wyświetli pytanie o ponowne uruchomienie systemu operacyjnego z określoną częstotliwością.

Domyślnie opcja ta jest włączona. Domyślnie przedział czasu wynosi 5 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

Jeśli ta opcja jest wyłączona, monit zostaje wyświetlony tylko raz.

- Uruchom ponownie po (min)

  Po wyświetleniu monitu, aplikacja wymusza ponowne uruchomienie systemu operacyjnego po minięciu określonego przedziału czasu.

  Domyślnie opcja ta jest włączona. Domyślne opóźnienie wynosi 30 minut. Dostępne wartości znajdują się w zakresie od 1 do 1440 minut.

- Czas oczekiwania przed wymuszeniem zamknięcia aplikacji dla zablokowanych sesji (min)

  Wymuszone zamknięcie aplikacji ma miejsce, gdy urządzenie użytkownika jest zablokowane (automatycznie po określonym czasie nieaktywności lub ręcznie).

  Jeśli ta opcja jest włączona, wymuszone zamknięcie aplikacji na zablokowanym urządzeniu odbywa się po minięciu czasu określonego w polu wejściowym.

  Jeśli ta opcja jest wyłączona, aplikacje nie będą zamykane na zablokowanym urządzeniu.

  Domyślnie opcja ta jest wyłączona.

8. Jeśli chcesz zmodyfikować domyślne ustawienia zadania, włącz opcję **Otwórz szczegóły zadania po jego utworzeniu** na stronie **Zakończ tworzenie zadania**. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

9. Kliknij przycisk **Zakończ**.

   Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

10. Kliknij nazwę utworzonego zadania, aby otworzyć okno właściwości zadania.

11. W oknie właściwości zadania określ ogólne ustawienia zadania zgodnie ze swoimi potrzebami.

12. Kliknij przycisk **Zapisz**.

    Zadanie zostało utworzone i skonfigurowane.

Jeśli wyniki zadania zawierają ostrzeżenie o błędzie 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", możesz rozwiązać ten problem poprzez Rejestr systemu Windows.

Dodawanie reguł dla instalacji aktualizacji

Ta funkcja jest dostępna tylko w ramach licencji na Zarządzanie lukami i poprawkami.

Podczas instalowania aktualizacji oprogramowania lub naprawiania luk w oprogramowaniu przy użyciu zadania *Zainstaluj wymagane aktualizacje i napraw luki* należy określić zasady instalacji aktualizacji. Te reguły określają aktualizacje do zainstalowania oraz luki do wyeliminowania.

Dokładne ustawienia zależą od tego, czy dodajesz regułę dla wszystkich aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich (aplikacje stworzone przez producentów oprogramowania innych niż Kaspersky i Microsoft) lub wszystkich aplikacji. Podczas dodawania reguły dla aktualizacji Windows Update lub aktualizacji aplikacji firm trzecich możesz wybrać określone aplikacje oraz wersje aplikacji, dla których chcesz zainstalować uaktualnienia. Podczas dodawani reguły dla wszystkich aktualizacji możesz wybrać określone uaktualnienia, które chcesz zainstalować, oraz luki, które chcesz wyeliminować poprzez zainstalowanie uaktualnień.

Regułę instalacji aktualizacji można dodać w następujący sposób:

- Dodając regułę podczas tworzenia nowego zadania Zainstaluj wymagane aktualizacje i napraw luki.
- Dodając regułę w zakładce **Ustawienia aplikacji** w oknie właściwości istniejącego zadania *Zainstaluj wymagane aktualizacje i napraw luki*.
- Za pomocą kreatora instalacji aktualizacji lub kreatora naprawiania luk.

W celu dodania nowej reguły dla wszystkich aktualizacji:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla wszystkich aktualizacji**.

3. W kroku **Kryteria ogólne** użyj list rozwijalnych do określenia następujących ustawień:

   - **Zbiór uaktualnień do zainstalowania**

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - **Napraw luki z priorytetem równym lub większym niż**

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aktualizacje** wybierz aktualizacje, które mają zostać zainstalowane:

   - **Zainstaluj wszystkie pasujące aktualizacje**

     Zainstaluj aktualizacje oprogramowania, które spełniają kryteria określone w kroku **Kryteria ogólne**. Ta opcja jest wybrana domyślnie.

   - **Zainstaluj tylko aktualizacje z listy**

     Instalowane są tylko te aktualizacje oprogramowania, które wybierzesz ręcznie z listy. Ta lista zawiera wszystkie dostępne aktualizacje oprogramowania.

     Na przykład, możesz wybrać określone aktualizacje w następujących przypadkach: aby sprawdzić ich instalację w środowisku testowym, aby zaktualizować tylko krytyczne aplikacje lub aby zaktualizować tylko określone aplikacje.

     - **Automatycznie zainstaluj wszystkie poprzednie aktualizacje aplikacji, jeśli są one niezbędne do zainstalowania wybranych aktualizacji**

       Pozostaw tę opcję włączoną, jeśli zgadzasz się na instalację tymczasowych wersji aplikacji, gdy jest to wymagane do zainstalowania wybranych aktualizacji.

       Jeśli ta opcja jest wyłączona, tylko wybrane wersje aplikacji są instalowane. Wybierz tę opcję, jeśli chcesz zaktualizować aplikacje w prosty sposób, bez próby zainstalowania kolejnych wersji. Jeśli zainstalowanie wybranych aktualizacji nie jest możliwe bez zainstalowania poprzednich wersji aplikacji, aktualizacja aplikacji nie powiedzie się.

       Na przykład, posiadasz wersję 3 aplikacji zainstalowanej na urządzeniu i chcesz zaktualizować ją do wersji 5, ale wersja 5 tej aplikacji może być zainstalowana tylko na wersji 4. Jeśli ta opcja jest włączona, oprogramowanie w pierwszej kolejności instaluje wersję 4, a następnie instaluje wersję 5. Jeśli ta opcja jest wyłączona, oprogramowanie nie zdoła zaktualizować aplikacji.

       Domyślnie opcja ta jest włączona.

5. W kroku **Luki** wybierz luki, które zostaną wyeliminowane poprzez zainstalowanie wybranych aktualizacji:

   - **Napraw wszystkie luki spełniające inne kryteria**

     Wyeliminuj wszystkie luki, które spełniają kryteria określone na stronie **Kryteria ogólne** kreatora. Ta opcja jest wybrana domyślnie.

   - **Napraw tylko luki z listy**

     Naprawione zostaną tylko te luki, które ręcznie wybierzesz z listy. Ta lista zawiera wszystkie wykryte luki.

     Na przykład, możesz wybrać określone luki w następujących przypadkach: aby sprawdzić ich eliminację w środowisku testowym, aby wyeliminować luki tylko w krytycznych aplikacjach lub aby wyeliminować luki tylko w określonych aplikacjach.

6. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

W celu dodania nowej reguły dla aktualizacji Windows Update:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji systemu Windows**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - Zbiór uaktualnień do zainstalowania

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - Napraw luki z priorytetem równym lub większym niż

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

   - Napraw luki z priorytetem MSRC równym lub większym niż

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez centrum Microsoft Security Response Center (MSRC) jest równy lub wyższy niż wartość wybrana na liście (**Niski**, **Średni, Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Kategorie aktualizacji** wybierz kategorie aktualizacji, które mają zostać zainstalowane. Te kategorie są takie same, jak w Microsoft Update Catalog. Domyślnie, zaznaczone są wszystkie kategorie.

6. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji **Ustawienia** okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

W celu dodania nowej reguły dla aktualizacji aplikacji firm trzecich:

1. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia reguły. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

2. Na stronie **Typ reguły** wybierz **Reguła dla aktualizacji firm trzecich**.

3. W oknie **Kryteria ogólne** określ następujące ustawienia:

   - Zbiór uaktualnień do zainstalowania

     Wybierz aktualizacje, które muszą być zainstalowane na urządzeniach klienckich:

     - **Zainstaluj tylko zatwierdzone aktualizacje**. Spowoduje to zainstalowanie tylko zatwierdzonych aktualizacji.
     - **Zainstaluj wszystkie aktualizacje (za wyjątkiem odrzuconych)**. Spowoduje to zainstalowanie aktualizacji posiadających stan *Zatwierdzono* lub *Nie zdefiniowano*.
     - **Zainstaluj wszystkie aktualizacje (wraz z odrzuconymi)**. Spowoduje to zainstalowanie wszystkich aktualizacji niezależnie od ich stanu zatwierdzenia. Tę opcję należy wybierać z rozwagą. Na przykład, użyj tej opcji, jeśli chcesz sprawdzić instalację niektórych odrzuconych aktualizacji w infrastrukturze testowej.

   - Napraw luki z priorytetem równym lub większym niż

     Czasami aktualizacje oprogramowania mogą wpłynąć ujemnie na doświadczenie użytkownika z oprogramowaniem. W takich przypadkach możesz zdecydować się na zainstalowanie tylko tych aktualizacji, które są krytyczne dla działania oprogramowania, a na pominięcie innych aktualizacji.

     Jeśli ta opcja jest włączona, aktualizacje eliminują tylko te luki, dla których priorytet określony przez Kaspersky jest równy lub wyższy niż wartość wybrana na liście (**Średni**, **Wysoki** lub **Krytyczny**). Luki z priorytetem niższym niż wybrana wartość nie zostają wyeliminowane.

     Jeśli ta opcja jest wyłączona, aktualizacje eliminują wszystkie luki niezależnie od ich priorytetu.

     Domyślnie opcja ta jest wyłączona.

4. W kroku **Aplikacje** wybierz aplikacje i wersje aplikacji, dla których chcesz zainstalować aktualizacje. Domyślnie, zaznaczone są wszystkie aplikacje.

5. W kroku **Nazwa** określ nazwę dla reguły, którą dodajesz. W późniejszym czasie możesz zmienić tę nazwę w sekcji Ustawienia okna właściwości utworzonego zadania.

Po zakończeniu działania kreatora tworzenia reguły, nowa reguła zostanie dodana i wyświetlona na liście reguł kreatora tworzenia nowego zadania lub we właściwościach zadania.

Wybieranie poprawek użytkownika dla luk w programach innych firm

Aby użyć zadania *Napraw luki*, należy ręcznie określić aktualizacje oprogramowania do naprawy luk w programach innych firm, wymienionych w ustawieniach zadania. Zadanie *Napraw luki* używa zalecanych poprawek dla oprogramowania firmy Microsoft oraz poprawek użytkownika dla innych programów innych firm. *Poprawki użytkownika* to aktualizacje oprogramowania do naprawy luk, które administrator ręcznie określa do zainstalowania.

W celu wybrania poprawek użytkownika dla luk w programach firm trzecich:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Luki w oprogramowaniu**.

   Strona wyświetla listę luk w oprogramowaniu wykrytych na urządzeniach klienckich.

2. Na liście luk w oprogramowaniu kliknij odnośnik z nazwą luki w oprogramowaniu, dla której chcesz określić poprawkę użytkownika.

   Zostanie otwarte okno właściwości luki.

3. W lewej części okna wybierz sekcję **Poprawki użytkownika i inne poprawki**.

   Zostanie wyświetlona lista poprawek użytkownika dla wybranej luki w oprogramowaniu.

4. Kliknij **Dodaj**.

   Zostanie wyświetlona lista dostępnych pakietów instalacyjnych. Lista wyświetlonych pakietów instalacyjnych odpowiada liście **Operacje → Repozytoria → Pakiety instalacyjne**. Jeśli nie utworzono pakietu instalacyjnego zawierającego poprawkę użytkownika dla wybranej luki, możesz utworzyć pakiet teraz, uruchamiając Kreator tworzenia nowego pakietu.

5. Wybierz pakiet (lub pakiety) instalacyjny zawierający poprawkę użytkownika (lub poprawki użytkownika) dla luki w oprogramowaniu innych firm.

6. Kliknij **Zapisz**.

   Zostaną określone pakiety instalacyjne zawierające poprawki użytkownika dla luki w oprogramowaniu. Jeśli zadanie jest uruchamiane *Napraw luki*, pakiet instalacyjny zostanie zainstalowany, a luka w oprogramowaniu zostanie wyeliminowana.

Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach

Po przeskanowaniu oprogramowaniu na zarządzanych urządzeniach w poszukiwaniu luk, możesz przejrzeć listę luk w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach.

W celu przejrzenia listy luk w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach:

W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Luki w oprogramowaniu**.

Strona wyświetla listę luk w oprogramowaniu wykrytych na urządzeniach klienckich.

Możesz także wygenerować i przejrzeć Raport o lukach.

Możesz określić filtr przeglądania listy luk w oprogramowaniu. Kliknij ikonę **Filtr** () w prawym górnym rogu listy luk w oprogramowaniu do zarządzania filtrem. Możesz także wybrać jeden z predefiniowanych filtrów z listy rozwijalnej **Wstępnie ustawione filtry** nad listą luk w oprogramowaniu.

Możesz uzyskać szczegółowe informacje o dowolnej luce z listy.

W celu uzyskania informacji o luce w oprogramowaniu:

Na liście luk w oprogramowaniu kliknij odnośnik z nazwą luki.

Zostanie otwarte okno właściwości luki w oprogramowaniu.

Przeglądanie informacji o lukach w oprogramowaniu wykrytych na wybranym zarządzanym urządzeniu

Możesz przejrzeć informacje o lukach w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu działającym pod kontrolą systemu Windows.

W celu przejrzenia listy luk w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, dla którego chcesz przejrzeć wykryte luki w oprogramowaniu.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.

3. W oknie właściwości wybranego urządzenia wybierz zakładkę **Zaawansowane**.

4. W lewej części okna wybierz sekcję **Luki w oprogramowaniu**.

   Jeśli chcesz przejrzeć tylko luki w oprogramowaniu, które mogą zostać wyeliminowane, wybierz opcję **Pokaż tylko luki, które można naprawić.**

Zostanie wyświetlona lista luk w oprogramowaniu, wykrytych na wybranym, zarządzanym urządzeniu.

W celu przejrzenia właściwości wybranej luki w oprogramowaniu:

Kliknij odnośnik z nazwą luki w oprogramowaniu na liście luk w oprogramowaniu.

Zostanie otwarte okno właściwości wybranej luki w oprogramowaniu.

Przeglądanie statystyk dotyczących luk na zarządzanych urządzeniach

Statystyki dla każdej luki w oprogramowaniu możesz przejrzeć na zarządzanych urządzeniach. Statystyki są przedstawiane w postaci wykresu. Wykres wyświetla liczbę urządzeń z następującymi stanami:

- *Zignorowano na: <liczba urządzeń>*. Stan jest przypisywany, jeśli we właściwościach luki ręcznie ustawiłeś opcję ignorowania luki.
- *Naprawiono na: <liczba urządzeń>*. Stan jest przypisywany, jeśli zadanie naprawy luki zostało zakończone pomyślnie.

- *Naprawa zaplanowana na: <liczba urządzeń>*. Stan jest przypisywany, jeśli utworzyłeś zadanie naprawy luki, ale zadanie nie zostało jeszcze wykonane.
- *Zastosowano poprawkę na: <liczba urządzeń>*. Stan jest przypisywany, jeśli ręcznie wybrałeś aktualizację oprogramowania do naprawy luki, ale ta aktualizacja oprogramowania nie usunęła luki.
- *Naprawa wymagana na: <liczba urządzeń>*. Stan jest przypisywany, jeśli luka została naprawiona tylko na części zarządzanych urządzeń, a wymagana jest jej naprawa na reszcie zarządzanych urządzeń.

W celu sprawdzenia statystyk dotyczących luki na zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Luki w oprogramowaniu**.

   Strona wyświetla listę luk w aplikacjach wykrytych na zarządzanych urządzeniach.

2. Zaznacz pole obok żądanej luki.
3. Kliknij przycisk **Statystyki luk na urządzeniach**.

   Zostanie wyświetlony wykres stanów luk. Kliknięcie stanu spowoduje otwarcie listy urządzeń, na których luka posiada wybrany stan.

Eksportowanie listy luk w oprogramowaniu do pliku

Wyświetloną listę luk możesz wyeksportować do plików CSV lub TXT. Możesz użyć tych plików, na przykład, do wysłania ich do swojego menedżera ds. bezpieczeństwa informacji lub przechowywać je w celach statystycznych.

W celu wyeksportowania listy luk w oprogramowaniu wykrytych na wszystkich zarządzanych urządzeniach do pliku tekstowy:

1. W menu głównym przejdź do **Operacje → Zarządzanie poprawkami → Luki w oprogramowaniu**.

   Strona wyświetla listę luk w aplikacjach wykrytych na zarządzanych urządzeniach.

2. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj wiersze do pliku TXT** lub przycisk **Eksportuj wiersze do pliku CSV**.

   Plik zawierający listę luk w oprogramowaniu zostanie pobrany na urządzenie, którego aktualnie używasz.

W celu wyeksportowania listy luk w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu, do pliku tekstowego:

1. Otwórz listę luk w oprogramowaniu wykrytych na wybranym zarządzanym urządzeniu.
2. Wybierz luki w oprogramowaniu, które chcesz wyeksportować.

   Pomiń ten krok, jeśli chcesz wyeksportować pełną listę luk w oprogramowaniu wykrytych na zarządzanym urządzeniu.

   Jeśli chcesz wyeksportować pełną listę luk w oprogramowaniu, wykrytych na zarządzanym urządzeniu, wyeksportowane zostaną tylko luki wyświetlane na bieżącej stronie.

3. W zależności od preferowanego formatu eksportowania, kliknij przycisk **Eksportuj wiersze do pliku TXT** lub przycisk **Eksportuj wiersze do pliku CSV**.

Plik zawierający listę luk w oprogramowaniu, wykrytych na wybranym zarządzanym urządzeniu, zostanie pobrany na urządzenie, którego używasz w danym momencie.

Ignorowanie luk w oprogramowaniu

Możesz zignorować luki w oprogramowaniu, które mają zostać naprawione. Przyczyny zignorowania luk w oprogramowaniu mogą być, na przykład, następujące:

- Nie uważasz luki w oprogramowaniu za krytyczną dla swojej organizacji.
- Rozumiesz, poprawka luki w oprogramowaniu może uszkodzić dane związane z oprogramowaniem, które wymagało naprawy luki.
- Jesteś pewien, że luka w oprogramowaniu nie jest niebezpieczna dla sieci w Twojej organizacji, ponieważ używasz innych środków ochrony swoich zarządzanych urządzeń.

Możesz zignorować lukę w oprogramowaniu na wszystkich zarządzanych urządzeniach lub tylko na wybranych zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wszystkich zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje** → **Zarządzanie poprawkami** → **Luki w oprogramowaniu**.

   Strona wyświetla listę luk w oprogramowaniu wykrytych na zarządzanych urządzeniach.

2. Na liście luk w oprogramowaniu kliknij odnośnik z nazwą luki w oprogramowaniu, którą chcesz zignorować.

   Zostanie otwarte okno właściwości luk w oprogramowaniu.

3. Na zakładce **Ogólne** włącz opcję **Ignoruj lukę**.

4. Kliknij przycisk **Zapisz**.

   Okno właściwości luk w oprogramowaniu zostanie zamknięte.

Luka w oprogramowaniu zostanie zignorowana na wszystkich zarządzanych urządzeniach.

W celu zignorowania luki w oprogramowaniu na wybranym zarządzanym urządzeniu:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.

2. Na liście zarządzanych urządzeń kliknij odnośnik z nazwą urządzenia, na którym chcesz zignorować lukę w oprogramowaniu.

   Zostanie otwarte okno właściwości urządzenia.

3. W oknie właściwości urządzenia wybierz zakładkę **Zaawansowane**.

4. W lewej części okna wybierz sekcję **Luki w oprogramowaniu**.

   Zostanie wyświetlona lista luk w oprogramowaniu wykrytych na urządzeniu.

5. Na liście luk w oprogramowaniu wybierz lukę, którą chcesz zignorować na wybranym urządzeniu.

   Zostanie otwarte okno właściwości luk w oprogramowaniu.

6. W oknie właściwości luki w oprogramowaniu, na zakładce **Ogólne** włącz opcję **Ignoruj lukę**.
7. Kliknij przycisk **Zapisz**.

   Okno właściwości luk w oprogramowaniu zostanie zamknięte.
8. Zamknij okno właściwości urządzenia.

Luka w oprogramowaniu zostanie zignorowana na wybranym urządzeniu.

Zignorowana luka w oprogramowaniu nie zostanie naprawiona po zakończeniu wykonywania zadania *Napraw luki* lub zadania *Zainstaluj wymagane aktualizacje i napraw luki*. Możesz wykluczyć zignorowane luki w oprogramowaniu z listy luk, korzystając z filtra.

Zarządzanie aplikacjami uruchomionymi na urządzeniach klienckich

Ta sekcja opisuje funkcje Kaspersky Security Center, które dotyczą zarządzania uruchamianiem aplikacji na urządzeniach klienckich.

Scenariusz: Zarządzanie aplikacjami

Możesz zarządzać uruchamianiem aplikacji na urządzeniach użytkowników. Możesz zezwolić na lub zablokować uruchamianie aplikacji na zarządzanych urządzeniach. Ta funkcjonalność jest realizowana przez komponent Kontrola aplikacji. Możesz zarządzać aplikacjami zainstalowanymi na urządzeniach z systemem Windows lub Linux.

W przypadku systemów operacyjnych opartych na systemie Linux komponent Kontrola aplikacji jest dostępny począwszy od Kaspersky Endpoint Security 11.2 for Linux.

Wymagania wstępne

- Kaspersky Security Center zostanie wdrożony w Twojej organizacji.
- Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Linux został utworzony i jest aktywny.

Etapy

Scenariusz korzystania z Kontroli aplikacji podzielony jest na etapy:

1. **Tworzenie i przeglądanie listy aplikacji na urządzeniach klienckich**

   Ten etap pomaga w odnalezieniu aplikacji, które są zainstalowane na zarządzanych urządzeniach. Możesz przejrzeć listę aplikacji i zdecydować, na które aplikacje chcesz zezwolić, a które chcesz zablokować zgodnie z polityką bezpieczeństwa organizacji. Ograniczenia mogą dotyczyć polityki bezpieczeństwa informacji, obowiązującej w Twojej organizacji. Możesz pominąć ten etap, jeśli wiesz dokładnie, jakie aplikacje są zainstalowane na zarządzanych urządzeniach.

   Dostępne instrukcje:

- Konsola administracyjna: Przeglądanie rejestru aplikacji
- Kaspersky Security Center Web Console: Uzyskiwanie i przeglądanie listy aplikacji zainstalowanych na urządzeniach klienckich

2. **Tworzenie i przeglądanie listy plików wykonywalnych na urządzeniach klienckich**

   Ten etap pomaga w odnalezieniu plików wykonywalnych, które znajdują się na zarządzanych urządzeniach. Przejrzyj listę plików wykonywalnych i porównaj ją z listami dozwolonych i zabronionych plików wykonywalnych. Ograniczenia dotyczące użycia plików wykonywalnych mogą być związane z polityką bezpieczeństwa informacji, obowiązującej w Twojej organizacji. Możesz pominąć ten etap, jeśli wiesz dokładnie, jakie pliki wykonywalne są zainstalowane na zarządzanych urządzeniach.

   Dostępne instrukcje:

   - Konsola administracyjna: Inwentaryzacja plików wykonywalnych
   - Kaspersky Security Center Web Console: Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

3. **Tworzenie kategorii aplikacji dla aplikacji używanych w Twojej organizacji**

   Przeanalizuj listy aplikacji i plików wykonywalnych, przechowywanych na zarządzanych urządzeniach. W oparciu o analizę, utwórz kategorie aplikacji. Zalecane jest utworzenie kategorii „Aplikacje do pracy", która obejmuje standardowy zestaw aplikacji używanych w Twojej organizacji. Jeśli różne grupy użytkowników używają różnych zestawów aplikacji w swojej pracy, oddzielna kategoria aplikacji może zostać utworzona dla każdej grupy użytkowników.

   W zależności od zestawu kryteriów do utworzenia kategorii aplikacji możesz utworzyć kategorie aplikacji trzech typów.

   Dostępne instrukcje:

   - Konsola administracyjna: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranych urządzeń, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranego folderu.
   - Kaspersky Security Center Web Console: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranych urządzeń, Tworzenie kategorii aplikacji, które zawierają pliki wykonywalne z wybranego folderu.

4. **Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security**

   Skonfiguruj komponent Kontrola aplikacji w zasadzie Kaspersky Endpoint Security, korzystając z kategorii aplikacji, które utworzono w poprzednim kroku.

   Dostępne instrukcje:

   - Konsola administracyjna: Konfigurowanie zarządzania uruchamianiem aplikacji na urządzeniach klienckich
   - Kaspersky Security Center Web Console: Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows

5. **Włączanie komponentu Kontrola aplikacji w trybie testowym**

   Aby zapewnić, że reguły Kontroli aplikacji nie będą blokowały aplikacji wymaganych do pracy użytkownika, zalecane jest włączenie testowania reguł Kontroli aplikacji i analizowanie ich działania po utworzeniu nowych reguł. Po włączeniu testowania, Kaspersky Endpoint Security for Windows nie zablokuje aplikacji, których uruchamianie jest zablokowane przez reguły Kontroli aplikacji, ale zamiast tego wyśle powiadomienia o ich uruchomieniu do Serwera administracyjnego.

   Podczas testowania reguł Kontroli aplikacji zalecane jest wykonanie następujących działań:

   - Określenie okresu testowania. Okres testowania może wahać się od siedmiu dni do dwóch miesięcy.

- Sprawdź zdarzenia wynikające z testowania działania Kontroli aplikacji.

Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i włącz opcję **Tryb testowy** w procesie konfiguracji.

6. **Zmienianie ustawień kategorii aplikacji komponentu Kontrola aplikacji**

   Jeśli to konieczne, wprowadź zmiany w ustawieniach Kontroli aplikacji. W oparciu o wyniki testu, możesz dodać pliki wykonywalne związane ze zdarzeniami komponentu Kontrola aplikacji do kategorii aplikacji z zawartością dodaną ręcznie.

   Dostępne instrukcje:

   - Konsola administracyjna: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji
   - Kaspersky Security Center Web Console: Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

7. **Stosowanie reguł Kontroli aplikacji w trybie działania**

   Po przetestowaniu reguł Kontroli aplikacji i zakończeniu konfiguracji kategorii aplikacji możesz zastosować reguły Kontroli aplikacji w trybie działania.

   Wskazówki jak postępować dla Kaspersky Security Center Web Console: Konfigurowanie komponentu Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Windows. Postępuj zgodnie z tymi instrukcjami i wyłącz opcję **Tryb testowy** w procesie konfiguracji.

8. **Weryfikowanie konfiguracji Kontroli aplikacji**

   Upewnij się, że wykonałeś następujące czynności:

   - Utworzyłeś kategorie aplikacji.
   - Skonfigurowałeś Kontrolę aplikacji przy użyciu kategorii aplikacji.
   - Zastosowałeś reguły Kontroli aplikacji w trybie działania.

Wyniki

Po zakończeniu scenariusza uruchamianie aplikacji na zarządzanych urządzeniach jest kontrolowane. Użytkownicy mogą uruchamiać tylko te aplikacje, które są dozwolone w Twojej organizacji, a nie mogą uruchamiać aplikacji, które są zabronione w Twojej organizacji.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Informacje o Kontroli aplikacji

Komponent Kontrola aplikacji monitoruje próby użytkowników mające na celu uruchomienie aplikacji i regulowanie uruchamiania aplikacji przy użyciu reguł Kontroli aplikacji.

Komponent Kontrola aplikacji jest dostępny dla Kaspersky Endpoint Security for Windows oraz dla Kaspersky Security for Virtualization Light Agent. Wszystkie instrukcje w tej sekcji opisują konfigurację Kontroli aplikacji dla Kaspersky Endpoint Security for Windows.

Uruchamianie aplikacji, których ustawienia nie odpowiadają żadnym regułom Kontroli aplikacji, jest regulowane przez wybrany tryb działania komponentu:

- *Lista blokowanych*. Tryb jest używany, jeśli chcesz zezwolić na uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji określonych w regułach blokowania. Ten tryb jest wybrany domyślnie.
- *Lista dozwolonych*. Tryb jest używany, jeśli chcesz zablokować uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji określonych w regułach zezwalania.

Reguły Kontroli aplikacji są implementowane poprzez kategorie aplikacji. Tworzysz kategorie aplikacji definiujące określone kryteria. W Kaspersky Security Center istnieją trzy typy kategorii aplikacji:

- Ręcznie dodana kategoria z zawartością. Definiujesz warunki, na przykład, metadane plików, wartość skrótu pliku, certyfikat pliku, kategorię KL, ścieżkę do pliku, aby uwzględniać pliki wykonywalne w kategorii.
- Kategoria zawierająca pliki wykonywalne z wybranych urządzeń. Określasz urządzenie, którego pliki wykonywalne są automatycznie uwzględniane w kategorii.
- Kategoria zawierająca pliki wykonywalne z wybranego folderu. Określasz folder, z którego pliki wykonywalne mają zostać automatycznie uwzględnione w kategorii.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Uzyskiwanie i przeglądanie listy aplikacji zainstalowanych na urządzeniach klienckich

Kaspersky Security Center przeprowadza inwentaryzację wszystkich programów zainstalowanych na zarządzanych urządzeniach klienckich działających pod kontrolą systemu Linux i Windows.

Agent sieciowy tworzy listę aplikacji zainstalowanych na urządzeniu, a następnie wysyła ją do Serwera administracyjnego. Aktualizacja listy aplikacji przez Agenta sieciowego zajmuje około 10–15 minut.

W przypadku urządzeń klienckich z systemem Windows Agent sieciowy otrzymuje większość informacji o zainstalowanych aplikacjach z rejestru systemu Windows. W przypadku urządzeń klienckich opartych na systemie Linux menedżery pakietów dostarczają Agentowi sieciowemu informacje o zainstalowanych aplikacjach.

W celu przejrzenia listy aplikacji zainstalowanych na zarządzanych urządzeniach:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Rejestr aplikacji**.

Strona wyświetla tabelę z aplikacjami zainstalowanymi na zarządzanych urządzeniach. Wybierz aplikację, aby wyświetlić jej właściwości, na przykład nazwę dostawcy, numer wersji, listę plików wykonywalnych, listę urządzeń, na których aplikacja jest zainstalowana, listę dostępnych aktualizacji oprogramowania oraz listę wykrytych luk w oprogramowaniu.

2. Możesz grupować i filtrować dane tabeli z zainstalowanymi aplikacjami w następujący sposób:

   - Kliknij ikonę ustawień ( ) w prawym górnym rogu tabeli.

     W wywołanym menu **Ustawienia kolumn** wybierz kolumny, które mają być wyświetlane w tabeli. Aby wyświetlić typ systemu operacyjnego urządzeń klienckich, na których zainstalowana jest aplikacja, wybierz kolumnę **Typ systemu operacyjnego**.

   - Kliknij ikonę filtra ( ) w prawym górnym rogu tabeli, a następnie określić i zastosować kryterium filtrowania w wywołanym menu.

     Zostanie wyświetlona przefiltrowana tabela zainstalowanych aplikacji.

Aby wyświetlić listę aplikacji zainstalowanych na określonym zarządzanym urządzeniu,

W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia** → **<nazwa urządzenia>** → **Zaawansowane** → **Rejestr aplikacji**. Z tego menu możesz wyeksportować listę aplikacji do pliku CSV lub pliku TXT.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

Możesz uzyskać listę plików wykonywalnych przechowywanych na zarządzanych urządzeniach. Aby przeprowadzić inwentaryzację plików wykonywalnych, należy utworzyć zadanie inwentaryzacji.

Funkcja inwentaryzacji plików wykonywalnych jest dostępna dla następujących aplikacji:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent i nowsze wersje

Możesz zmniejszyć obciążenie bazy danych, jednocześnie uzyskując informacje o zainstalowanych aplikacjach. W tym celu zalecamy uruchomienie zadania inwentaryzacji na urządzeniach referencyjnych, na których jest zainstalowany standardowy zestaw oprogramowania.

W celu utworzenia zadania dla plików wykonywalnych na urządzeniach klienckich:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.

   Zostanie wyświetlona lista zadań.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania. Postępuj zgodnie z krokami kreatora.

3. Na stronie **Nowe zadanie**, z listy rozwijanej **Aplikacja** wybierz Kaspersky Endpoint Security for Windows lub Kaspersky Endpoint Security for Linux, w zależności od typu systemu operacyjnego urządzeń klienckich.

4. Z listy rozwijalnej **Typ zadania** wybierz **Inwentaryzacja**.

5. Na stronie **Zakończ tworzenie zadania** kliknij przycisk **Zakończ**.

   Po zakończeniu działania Kreatora tworzenia nowego zadania, zostaje utworzone i skonfigurowane zadanie **Inwentaryzacja**. Jeśli chcesz, możesz zmienić ustawienia dla utworzonego zadania. Nowo utworzone zadanie będzie wyświetlane na liście zadań.

Szczegółowy opis zadania inwentaryzacji znajduje się w następujących Pomocach:

- Pomoc Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux — pomoc
- Kaspersky Security for Virtualization Light Agent

Po wykonaniu zadania **Inwentaryzacja**, zostaje utworzona lista plików wykonywalnych przechowywanych na zarządzanych urządzeniach i możesz przejrzeć listę.

Podczas inwentaryzacji wykrywane są pliki wykonywalne w następujących formatach: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR oraz HTML.

W celu przejrzenia listy plików wykonywalnych przechowywanych na urządzeniach klienckich:

W menu głównym przejdź do **Operacje → Aplikacje innych firm → Pliki wykonywalne**.

Strona wyświetla listę plików wykonywalnych przechowywanych na urządzeniach klienckich.

W celu wysłania pliku wykonywalnego z zarządzanego urządzenia do Kaspersky:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Pliki wykonywalne**.

2. Kliknij odnośnik do pliku wykonywalnego, który chcesz wysłać do Kaspersky.

3. W oknie, które zostanie otwarte, przejdź do sekcji **Urządzenia**, a następnie zaznacz pole wyboru zarządzanego urządzenia, z którego chcesz wysłać plik wykonywalny.

   Przed wysłaniem pliku wykonywalnego upewnij się, że zarządzane urządzenie ma bezpośrednie połączenie z Serwerem administracyjnym, zaznaczając pole **Nie odłączaj od Serwera administracyjnego**.

4. Kliknij przycisk **Wyślij do firmy Kaspersky**.

Wybrany plik wykonywalny jest pobierany w celu dalszego wysłania do Kaspersky.

Tworzenie kategorii aplikacji z zawartością dodaną ręcznie

Możesz określić zestaw kryteriów jako szablon plików wykonywalnych, dla których chcesz zezwolić na lub zablokować uruchamianie w Twojej organizacji. W oparciu o pliki wykonywalne odpowiadające kryteriom, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji z zawartością dodaną ręcznie:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii aplikacji.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Postępuj zgodnie z krokami kreatora.

3. W kroku **Wybierz metodę tworzenia kategorii** kreatora wybierz opcję **Kategoria z zawartością dodaną ręcznie. Dane plików wykonywalnych są dodawane do tej kategorii ręcznie**.

4. W kroku **Warunki** kliknij przycisk **Dodaj**, aby dodać kryterium warunku do uwzględnienia plików w tworzonej kategorii.

5. W kroku **Kryteria warunku** wybierz typ reguły dla tworzenia kategorii z listy:

   - Z kategorii KL

     Jeśli ta opcja jest zaznaczona, możesz określić kategorię aplikacji Kaspersky jako warunek dodania aplikacji do kategorii użytkownika. Aplikacje z określonej kategorii Kaspersky zostaną dodane do kategorii użytkownika dla aplikacji.

   - Wybierz certyfikat z repozytorium

     Jeśli ta opcja jest zaznaczona, możesz określić certyfikaty z repozytorium. Pliki wykonywalne, które zostały podpisane zgodnie z określonymi certyfikatami, zostaną dodane do kategorii użytkownika.

   - Określ ścieżkę do aplikacji (maski są obsługiwane)

     Jeżeli ta opcja zostanie zaznaczona, możesz określić ścieżkę do folderu na urządzeniu klienckim zawierający pliki wykonywalne, które zostaną dodane do kategorii użytkownika dla aplikacji.

   - Dysk wymienny

     Jeżeli ta opcja jest zaznaczona, możesz określić typ nośnika (dowolne urządzenie lub urządzenie przenośne), na którym aplikacja jest uruchomiona. Aplikacje, które były uruchomione na wybranym typie urządzenia, zostaną dodane do kategorii użytkownika dla aplikacji.

   - **Suma kontrolna, metadane lub certyfikat**:

     - Wybierz z listy plików wykonywalnych

Jeśli ta opcja jest zaznaczona, możesz wskazać na liście plików wykonywalnych na urządzeniu klienckim te aplikacje, które chcesz dodać do kategorii.

- **Wybierz z rejestru aplikacji**

  Jeśli ta opcja jest wybrana, zostanie wyświetlony rejestr aplikacji. Możesz wybrać aplikację z rejestru i określić następujące metadane plików:

  - Nazwa pliku.
  - Wersja pliku. Możesz określić dokładną wartość wersji lub opisać warunek, na przykład „większy niż 5.0”.
  - Nazwa aplikacji.
  - Wersja aplikacji. Możesz określić dokładną wartość wersji lub opisać warunek, na przykład „większy niż 5.0”.
  - Producent.

- **Określ ręcznie**

Jeśli ta opcja jest zaznaczona, możesz określić sumę kontrolną pliku lub metadane lub certyfikat jako warunek dodawania aplikacji do kategorii użytkownika.

Suma kontrolna pliku

W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o obliczonych wartościach sum kontrolnych są przechowywane w bazie danych Serwera administracyjnego. Przechowywanie wartości sum kontrolnych nie zwiększa znacząco rozmiaru bazy danych.

SHA-256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono usterek, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA-256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA-256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA-256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

- Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego, dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA-256 dla plików kategorii.

- Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA-256**, jak i pole wyboru **Suma kontrolna MD5**.

Metadane

Jeśli ta opcja jest wybrana, możesz określić metadane pliku jako nazwę pliku, wersję pliku, producenta. Metadane zostaną przesłane do Serwera administracyjnego. Pliki wykonywalne, które zawierają te same metadane, zostaną dodane do kategorii aplikacji.

Certyfikat

Jeśli ta opcja jest zaznaczona, możesz określić certyfikaty z repozytorium. Pliki wykonywalne, które zostały podpisane zgodnie z określonymi certyfikatami, zostaną dodane do kategorii użytkownika.

- Z pliku lub z pakietu MSI / zarchiwizowanego folderu

Jeśli ta opcja jest zaznaczona, możesz określić plik instalatora MSI jako warunek dodania aplikacji do kategorii użytkownika. Metadane instalatora aplikacji zostaną przesłane do Serwera administracyjnego. Aplikacje, dla których metadane instalatora są takie same jak dla określonego instalatora MSI, zostaną dodane do kategorii użytkownika dla aplikacji.

Wybrane kryterium zostanie dodane do listy warunków.

Możesz dodać tyle kryteriów tworzenia kategorii aplikacji, ile potrzebujesz.

6. W kroku **Wykluczenia** kliknij przycisk **Dodaj**, aby dodać kryterium warunku wykluczenia w celu wykluczenia plików z tworzonej kategorii.

7. W kroku **Kryteria warunku** wybierz typ reguły z listy w taki sam sposób, w jaki wybierałeś typ reguły dla tworzenia kategorii.

Jeśli kreator zakończy działanie, zostanie utworzona kategoria aplikacji. Jest wyświetlana na liście kategorii aplikacji. Po skonfigurowaniu Kontroli aplikacji możesz użyć utworzonej kategorii aplikacji.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń

Możesz użyć plików wykonywalnych z wybranych urządzeń jako szablonu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić. W oparciu o pliki wykonywalne z wybranych urządzeń, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji, która zawiera pliki wykonywalne z wybranych urządzeń:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii aplikacji.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku Next.

3. W kroku **Wybierz metodę tworzenia kategorii** kreatora określ nazwę kategorii i wybierz opcję **Kategoria zawierająca pliki wykonywalne znajdujące się na wybranych urządzeniach. Takie pliki wykonywalne są przetwarzane automatycznie, a ich metryki są dodawane do kategorii**.

4. Kliknij **Dodaj**.

5. W otwartym oknie wybierz urządzenie lub urządzenia, których pliki wykonywalne będą używane do tworzenia kategorii aplikacji.

6. Określ następujące ustawienia:

   - Algorytm obliczania wartości sumy kontrolnej

W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o obliczonych wartościach sum kontrolnych są przechowywane w bazie danych Serwera administracyjnego. Przechowywanie wartości sum kontrolnych nie zwiększa znacząco rozmiaru bazy danych.

SHA-256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono usterek, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA-256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA-256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA-256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

- Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego, dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA-256 dla plików kategorii.

Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA-256**, jak i pole wyboru **Suma kontrolna MD5**.

Pole **Oblicz sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze)** jest zaznaczone domyślnie.

Pole **Przelicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

- Synchronizuj dane z repozytorium Serwera administracyjnego

Wybierz tę opcję, jeśli chcesz, żeby Serwer administracyjny okresowo sprawdzał zmiany w określonym folderze (lub folderach).

Domyślnie opcja ta jest wyłączona.

Jeśli włączysz tę opcję, określ przedział czasu (w godzinach), aby sprawdzić zmiany w określonym folderze (folderach). Domyślnie przedział czasu skanowania wynosi 24 godziny.

- Typ pliku

W tej sekcji możesz określić typ pliku, który jest używany do tworzenia kategorii aplikacji.

Wszystkie pliki. Wszystkie pliki są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

Tylko pliki spoza kategorii aplikacji. Tylko pliki poza kategoriami aplikacji są brane pod uwagę podczas tworzenia kategorii.

- Foldery

W tej sekcji możesz określić, które foldery z wybranego urządzenia (urządzeń) zawierają pliki używane do tworzenia kategorii aplikacji.

Wszystkie foldery. Wszystkie foldery są brane pod uwagę podczas tworzenia kategorii. Domyślnie opcja ta jest zaznaczona.

Określony folder. Tylko określony folder jest brany pod uwagę podczas tworzenia kategorii. Jeśli wybierzesz tę opcję, musisz określić ścieżkę do folderu.

Jeśli kreator zakończy działanie, zostanie utworzona kategoria aplikacji. Jest wyświetlana na liście kategorii aplikacji. Po skonfigurowaniu Kontroli aplikacji możesz użyć utworzonej kategorii aplikacji.

Tworzenie kategorii aplikacji, która zawiera pliki wykonywalne z wybranego folderu

Możesz użyć plików wykonywalnych z wybranego folderu jako standardu plików wykonywalnych, które chcesz zablokować lub na które chcesz zezwolić w swojej organizacji. W oparciu o pliki wykonywalne z wybranego folderu, możesz utworzyć kategorię aplikacji i użyć jej w konfiguracji komponentu Kontrola aplikacji.

W celu utworzenia kategorii aplikacji, która zawiera pliki wykonywalne z wybranego folderu:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Kategorie aplikacji**.

   Zostanie wyświetlona strona z listą kategorii aplikacji.

2. Kliknij przycisk **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

3. W kroku **Wybierz metodę tworzenia kategorii** kreatora określ nazwę kategorii i wybierz opcję **Kategoria, która zawiera pliki wykonywalne z określonego folderu. Pliki wykonywalne aplikacji skopiowane do określonego folderu są przetwarzane automatycznie, a ich metryki są dodawane do kategorii**.

4. Określ folder, którego pliki wykonywalne zostaną użyte do utworzenia kategorii aplikacji.

5. Określ następujące ustawienia:

   - **Uwzględnij w tej kategorii biblioteki dołączane dynamicznie (DLL)**

     Kategoria aplikacji zawiera biblioteki dołączane dynamicznie (pliki w formacie DLL), a moduł Kontrola aplikacji rejestruje akcje takich bibliotek działających w systemie. Włączenie plików DLL do kategorii może obniżyć wydajność Kaspersky Security Center.

     Domyślnie pole to nie jest zaznaczone.

   - **Uwzględnij w tej kategorii dane skryptów**

     Kategoria aplikacji zawiera dane o skryptach, a skrypty nie są blokowane przez moduł Ochrona WWW. Włączenie danych skryptów do kategorii może obniżyć wydajność Kaspersky Security Center.

     Domyślnie pole to nie jest zaznaczone.

- Algorytm obliczania wartości sumy kontrolnej: **Oblicz sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze) / Oblicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane przez starsze wersje niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

  W zależności od wersji aplikacji zabezpieczającej, zainstalowanej na urządzeniach w sieci, musisz wybrać algorytm obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w tej kategorii. Informacje o obliczonych wartościach sum kontrolnych są przechowywane w bazie danych Serwera administracyjnego. Przechowywanie wartości sum kontrolnych nie zwiększa znacząco rozmiaru bazy danych.

  SHA-256 jest kryptograficzną funkcją skrótu: w algorytmie nie znaleziono usterek, dlatego jest obecnie najbardziej aktualną funkcją kryptograficzną. Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze wersje obsługują obliczanie SHA-256. Obliczanie funkcji skrótu MD5 jest obsługiwane przez wszystkie wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

  Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center dla plików w kategorii:

  - Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowanych w Twojej sieci to Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowsze wersje, zaznacz pole **SHA-256**. Nie zaleca się dodawania dowolnych kategorii utworzonych zgodnie z kryterium sumy kontrolnej SHA-256 pliku wykonywalnego dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Może to spowodować błędy w działaniu aplikacji zabezpieczającej. W takim przypadku można użyć kryptograficznej funkcji skrótu MD5 dla plików kategorii.

  - Jeśli w Twojej sieci są zainstalowane wersje wcześniejsze niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, wybierz **Suma kontrolna MD5**. Nie można dodać kategorii, która została utworzona na podstawie kryterium sumy kontrolnej MD5 pliku wykonywalnego, dla Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub nowszych wersji. W takim przypadku można użyć kryptograficznej funkcji skrótu SHA-256 dla plików kategorii.

  Jeśli różne urządzenia w Twojej sieci używają zarówno wcześniejszych, jak i nowszych wersji Kaspersky Endpoint Security 10, zaznacz zarówno pole **SHA-256**, jak i pole wyboru **Suma kontrolna MD5**.

  Pole **Oblicz sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze)** jest zaznaczone domyślnie.

  Pole **Przelicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane w wersjach starszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** jest odznaczone domyślnie.

- Wymuś skanowanie folderu pod kątem zmian

  Jeśli ta opcja jest włączona, aplikacja regularnie sprawdza folder dodawania zawartości kategorii na obecność zmian. Możesz określić częstotliwość skanowań (w godzinach) w polu wejściowym znajdującym się obok pola do zaznaczenia. Domyślnie przedział czasu między wymuszonymi skanowaniami wynosi 24 godziny.

  Jeśli ta opcja jest wyłączona, aplikacja nie wymusza skanowania folderu. Serwer podejmie próbę uzyskania dostępu do plików, jeśli zostały zmodyfikowane, dodane lub usunięte.

  Domyślnie opcja ta jest wyłączona.

Jeśli kreator zakończy działanie, zostanie utworzona kategoria aplikacji. Jest wyświetlana na liście kategorii aplikacji. Podczas konfiguracji Kontroli aplikacji możesz użyć kategorii aplikacji.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux

- Kaspersky Security for Virtualization Light Agent

Przeglądanie listy kategorii aplikacji

Możesz przejrzeć listę konfigurowanych kategorii aplikacji i ustawień każdej kategorii aplikacji.

W celu przejrzenia listy kategorii aplikacji:

W menu głównym przejdź do **Operacje** → **Aplikacje innych firm** → **Kategorie aplikacji**.

Zostanie wyświetlona strona z listą kategorii aplikacji.

W celu przejrzenia właściwości kategorii aplikacji:

Kliknij nazwę kategorii aplikacji.

Zostanie wyświetlone okno właściwości kategorii aplikacji. Właściwości zostaną pogrupowane na kilku zakładkach.

Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows

Po utworzeniu kategorii Kontroli aplikacji możesz użyć ich do konfigurowania Kontroli aplikacji w zasadach Kaspersky Endpoint Security for Windows.

W celu skonfigurowania Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Windows:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.

   Zostanie wyświetlona lista zasad.

2. Kliknij zasadę **Kaspersky Endpoint Security for Windows**.

   Zostanie otwarte okno ustawień zasady.

3. Przejdź do **Ustawienia aplikacji** → **Kontrola bezpieczeństwa** → Kontrola **aplikacji**.

   Zostanie wyświetlone okno **Kontrola aplikacji** z ustawieniami Kontroli aplikacji.

4. Opcja **Kontrola aplikacji** jest domyślnie włączona. Upewnij się, że przycisk przełączania **WYŁĄCZONA Kontrola aplikacji** jest ustawiony w pozycji wyłączonej.

5. W ustawieniach blokowania **Ustawienia Kontroli aplikacji** włącz tryb działania, aby zastosować reguły Kontroli aplikacji i zezwól Kaspersky Endpoint Security for Windows na blokowanie uruchamiania aplikacji.

   Jeśli chcesz przetestować reguły Kontroli aplikacji, w sekcji **Ustawienia Kontroli aplikacji** włącz tryb testowy. W trybie testowym Kaspersky Endpoint Security for Windows nie blokuje uruchamiania aplikacji, ale rejestruje informacje o wyzwolonych regułach w raporcie. Kliknij łącze **Wyświetl raport**, aby wyświetlić te informacje.

6. Włącz opcję **Kontrola wczytywania modułów DLL**, jeśli chcesz, żeby program Kaspersky Endpoint Security for Windows monitorował wczytywanie modułów DLL, gdy aplikacje są uruchamiane przez użytkowników.

   Informacje o module i aplikacji, która wczytuje moduł, zostaną zapisane w raporcie.

Kaspersky Endpoint Security for Windows monitoruje tylko moduły DLL i sterowniki wczytywane po wybraniu opcji **Kontrola wczytywania modułów DLL**. Uruchom ponownie komputer po wybraniu opcji **Kontrola wczytywania modułów DLL**, jeśli chcesz, żeby program Kaspersky Endpoint Security for Windows monitorował wszystkie moduły DLL i sterowniki, w tym te wczytywane przed uruchomieniem Kaspersky Endpoint Security for Windows.

7. (Opcjonalne) W sekcji **Szablony wiadomości** zmień szablon wiadomości,która jest wyświetlana po zablokowaniu możliwości uruchomienia aplikacji, oraz szablon wiadomości e-mail, która jest wysyłana do Ciebie.

8. W ustawieniach sekcji **Tryb Kontroli aplikacji** wybierz tryb **Lista blokowanych** lub **Lista dozwolonych**.

   Domyślnie, wybrany jest tryb **Lista blokowanych**.

9. Kliknij odnośnik **Ustawienia list reguł**.

   Zostanie otwarte okno **Lista blokowanych i lista dozwolonych**, w którym można dodać kategorię aplikacji. Domyślnie, wybrana jest zakładka **Lista blokowanych**, jeśli wybrany jest tryb **Lista blokowanych** lub wybrana jest zakładka **Lista dozwolonych**, jeśli wybrany jest tryb **Lista dozwolonych**.

10. W oknie **Lista blokowanych i lista dozwolonych** kliknij przycisk **Dodaj**.

    Zostanie otwarte okno **Reguła Kontroli aplikacji**.

11. Kliknij łącze **Wybierz kategorię**.

    Zostanie otwarte okno **Kategoria aplikacji**.

12. Dodaj kategorię (lub kategorie) aplikacji, które utworzyłeś wcześniej.

    Możesz edytować ustawienia utworzonej kategorii, klikając przycisk **Edytuj**.

    Możesz utworzyć nową kategorię, klikając przycisk **Dodaj**.

    Możesz usunąć kategorię z listy, klikając przycisk **Usuń**.

13. Po zakończeniu tworzenia listy kategorii aplikacji, kliknij przycisk **OK**.

    Okno **Kategoria aplikacji** zostanie zamknięte.

14. W oknie reguły **Kontrola aplikacji**, w sekcji **Użytkownicy i ich uprawnienia** utwórz listę użytkowników i grup użytkowników do zastosowania reguły Kontroli aplikacji.

15. Aby zapisać ustawienia i zamknąć okno **Reguła Kontroli aplikacji**, kliknij przycisk **OK**.

16. Aby zapisać ustawienia i zamknąć okno **Lista blokowanych i lista dozwolonych**, kliknij przycisk **OK**.

17. Aby zapisać ustawienia i zamknąć okno **Kontrola aplikacji**, kliknij przycisk **OK**.

18. Zamknij okno z ustawieniami profilu Kaspersky Endpoint Security for Windows.

Kontrola aplikacji została skonfigurowana. Po przeniesieniu zasady na urządzenia klienckie, możliwe jest zarządzanie uruchamianiem plików wykonywalnych.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

Po skonfigurowaniu Kontroli aplikacji w zasadach Kaspersky Endpoint Security for Windows, na liście zdarzeń zostaną wyświetlone następujące zdarzenia:

- **Zablokowano uruchomienie aplikacji** (zdarzenie *Krytyczne*). To zdarzenie jest wyświetlane, jeśli skonfigurowałeś Kontrolę aplikacji do stosowania reguł.
- **Zablokowane uruchomienie aplikacji w trybie testowym** (zdarzenie *Informacje*). To zdarzenie jest wyświetlane, jeśli skonfigurowałeś Kontrolę aplikacji do testowania reguł.
- **Wiadomość o zablokowaniu uruchomienia aplikacji do administratora** (zdarzenie *Ostrzeżenie*). To zdarzenie jest wyświetlane, jeśli skonfigurowałeś Kontrolę aplikacji do stosowania reguł i użytkownik zażądał dostępu do aplikacji, która jest zablokowana podczas uruchamiania.

Zalecane jest utworzenie wyborów zdarzeń, aby przeglądać zdarzenia dotyczące działania Kontroli aplikacji.

Możesz dodać pliki wykonywalne dotyczące zdarzeń Kontroli aplikacji do istniejącej kategorii aplikacji lub do nowej kategorii aplikacji. Możesz dodać pliki wykonywalne tylko do kategorii aplikacji z zawartością dodaną ręcznie.

W celu dodania plików wykonywalnych związanych ze zdarzeniami Kontroli aplikacji do kategorii aplikacji:

1. W menu głównym przejdź do **Monitorowanie i raportowanie → Wybory zdarzeń**.

   Zostanie wyświetlona lista wyborów zdarzeń.

2. Wybierz wybór zdarzeń, aby przeglądać zdarzenia związane z Kontrolą aplikacji oraz uruchomić ten wybór zdarzeń.

   Jeśli nie utworzyłeś wyboru zdarzeń dotyczącego Kontroli aplikacji, możesz wybrać i uruchomić predefiniowany wybór, na przykład, **Ostatnie zdarzenia**.

   Zostanie wyświetlona lista zdarzeń.

3. Wybierz zdarzenia, których skojarzone pliki wykonywalne chcesz dodać do kategorii aplikacji, a następnie kliknij przycisk **Przypisz do kategorii**.

   Zostanie uruchomiony Kreator tworzenia nowej kategorii. Przejdź przez kroki kreatora, korzystając z przycisku **Next**.

4. W kroku kreatora określ odpowiednie ustawienia:

   - W sekcji **Akcja na pliku wykonywalnym związanym ze zdarzeniem** wybierz jedną z następujących opcji:

     - Dodaj do nowej kategorii aplikacji

       Wybierz tę opcję, jeśli chcesz utworzyć nową kategorię aplikacji w oparciu o pliki wykonywalne dotyczące zdarzeń.

       Domyślnie opcja ta jest zaznaczona.

       Jeśli wybrałeś tę opcję, określ nową nazwę kategorii.

     - Dodaj do istniejącej kategorii aplikacji

Wybierz tę opcję, jeśli chcesz dodać pliki wykonywalne dotyczące zdarzeń do istniejącej kategorii aplikacji.

Domyślnie ta opcja nie jest zaznaczona.

Jeśli wybrałeś tę opcję, wybierz kategorię aplikacji z zawartością dodaną ręcznie, do której chcesz dodać pliki wykonywalne.

- W sekcji **Typ reguły** wybierz jedną z następujących opcji:
  - **Reguły dodawania do włączeń**
  - **Reguły dodawania do wykluczeń**
- W sekcji **Parametr użyty jako warunek** wybierz jedną z następujących opcji:
  - Szczegóły certyfikatu (lub sumy kontrolne SHA-256 dla plików bez certyfikatu)

    Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

    Każdy plik posiada swoją unikatową funkcję skrótu SHA-256. Jeśli wybierzesz funkcję skrótu SHA-256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać do reguł kategorii szczegóły certyfikatu pliku wykonywalnego (lub funkcję skrótu SHA-256 dla plików bez certyfikatu).

    Domyślnie opcja ta jest zaznaczona.

  - Szczegóły certyfikatu (pliki bez certyfikatu zostaną pominięte)

    Pliki mogą być podpisane certyfikatem. Kilka plików może być podpisanych tym samym certyfikatem. Na przykład, różne wersje tej samej aplikacji mogą być podpisane tym samym certyfikatem lub kilka różnych aplikacji od tego samego producenta może być podpisanych tym samym certyfikatem. Jeśli wybierzesz certyfikat, kilka wersji aplikacji lub kilka aplikacji od tego samego producenta może zostać przydzielonych do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać szczegóły certyfikatu pliku wykonywalnego do reguł kategorii. Jeśli plik wykonywalny nie posiada certyfikatu, ten plik zostanie pominięty. Do kategorii nie zostaną dodane żadne informacje o tym pliku.

  - Tylko SHA-256 (pliki bez sumy kontrolnej zostaną pominięte)

    Każdy plik posiada swoją unikatową funkcję skrótu SHA-256. Jeśli wybierzesz funkcję skrótu SHA-256, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

    Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu SHA-256 pliku wykonywalnego.

  - Tylko MD5 (tryb wycofany, wyłącznie dla wersji Kaspersky Endpoint Security 10 Service Pack 1)

Każdy plik posiada swoją unikatową funkcję skrótu MD5. Jeśli wybierzesz funkcję skrótu MD5, tylko jeden odpowiadający plik, na przykład, zdefiniowana wersja aplikacji, zostanie przydzielony do kategorii.

Wybierz tę opcję, jeśli chcesz dodać tylko szczegóły funkcji skrótu MD5 pliku wykonywalnego. Obliczanie funkcji skrótu MD5 jest obsługiwane w Kaspersky Endpoint Security 10 Service Pack 1 for Windows i późniejszych wersjach.

5. Kliknij **OK**.

Jeśli kreator zakończy działanie, pliki wykonywalne dotyczące zdarzeń Kontroli aplikacji są dodawane do istniejącej kategorii aplikacji lub do nowej kategorii aplikacji. Możesz przejrzeć ustawienia kategorii aplikacji, które zmodyfikowałeś lub utworzyłeś.

Aby uzyskać szczegółowe informacje na temat Kontroli aplikacji, zapoznaj się z następującymi tematami Pomocy:

- Pomoc Online Kaspersky Endpoint Security for Windows
- Pomoc Online Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Tworzenie pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Kaspersky Security Center Web Console pozwala na zdalną instalację aplikacji firm trzecich przy użyciu pakietów instalacyjnych. Takie aplikacje innych firm są zawarte w dedykowanej bazie danych Kaspersky. Baza danych jest tworzona automatycznie, gdy uruchamiasz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* po raz pierwszy.

W celu utworzenia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**.
2. Kliknij przycisk **Dodaj**.
3. Na otwartej stronie Kreatora nowego pakietu wybierz opcję **Wybierz aplikację z bazy danych Kaspersky do utworzenia pakietu instalacyjnego**, a następnie kliknij **Dalej**.
4. Na liście aplikacji, która zostanie otwarta, wybierz odpowiednią aplikację, a następnie kliknij **Dalej**.
5. Wybierz odpowiedni język lokalizacji z listy rozwijanej, a następnie kliknij **Dalej**.

Ten krok jest wyświetlany tylko wtedy, gdy aplikacja umożliwia wybór opcji językowych.

6. Jeśli pojawi się monit o zaakceptowanie umowy licencyjnej na instalację, na stronie **Umowa licencyjna użytkownika końcowego**, która zostanie otwarta, kliknij odnośnik, aby przeczytać umowę licencyjną w witrynie internetowej dostawcy, a następnie wybierz pole wyboru **Potwierdzam, że w pełni przeczytałem, rozumiem i akceptuję warunki oraz postanowienia tej Umowy licencyjnej użytkownika końcowego**.

7. Na stronie **Nazwa nowego pakietu instalacyjnego**, która zostanie otwarta, w polu **Nazwa pakietu** wprowadź nazwę pakietu instalacyjnego i kliknij **Dalej**.

Poczekaj, aż nowo utworzony pakiet instalacyjny zostanie przesłany na Serwer administracyjny. Jeśli Kreator tworzenia nowego pakietu wyświetla wiadomość informującą, że proces tworzenia pakietu zakończył się pomyślnie, kliknij **Zakończ**.

Nowo utworzony pakiet instalacyjny pojawi się na liście pakietów instalacyjnych. Możesz wybrać ten pakiet podczas tworzenia lub ponownego konfigurowania zadania *Zdalna instalacja aplikacji*.

Przeglądanie i modyfikowanie ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Jeśli poprzednio utworzyłeś jakiekolwiek pakiety instalacyjne aplikacji innych firm znajdujące się w bazie danych Kaspersky, możesz przejrzeć i zmodyfikować ustawienia tych pakietów.

Modyfikowanie ustawień pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky jest dostępne tylko w licencji Zarządzanie lukami i poprawkami.

W celu przejrzenia i zmodyfikowania ustawień pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Pakiety instalacyjne**.
2. Na otwartej liście pakietów instalacyjnych kliknij nazwę odpowiedniego pakietu.
3. Na otwartej stronie właściwości zmodyfikuj ustawienia (jeśli jest to konieczne).
4. Kliknij przycisk **Zapisz**.

Zmodyfikowane ustawienia zostaną zapisane.

Ustawienia pakietu instalacyjnego aplikacji innej firmy z bazy danych Kaspersky

Ustawienia pakietu instalacyjnego aplikacji innej firmy są pogrupowane na następujących zakładkach:

Tylko część ustawień wymienionych poniżej jest wyświetlana domyślnie, więc możesz dodać odpowiednie kolumny, klikając przycisk **Filtr** i wybierając nazwy odpowiednich kolumn z listy.

- Zakładka **Ogólne**:
  - Pole wejściowe które zawiera nazwę pakietu instalacyjnego, który może zostać edytowany ręcznie
  - Aplikacja

    Nazwa aplikacji innej firmy, dla której tworzony jest pakiet instalacyjny.

- **Wersja**

  Numer wersji aplikacji innej firmy, dla której tworzony jest pakiet instalacyjny.

- **Rozmiar**

  Rozmiar pakietu instalacyjnego innej firmy (w kilobajtach).

- **Utworzono**

  Data i godzina utworzenia pakietu instalacyjnego innej firmy.

- **Ścieżka dostępu**

  Ścieżka do folderu sieciowego, w którym przechowywany jest pakiet instalacyjny innej firmy.

- Zakładka **Procedura instalacji**:

  - **Zainstaluj wymagane ogólne składniki systemu**

    Jeśli ta opcja jest włączona, przed zainstalowaniem aktualizacji aplikacja automatycznie instaluje wszystkie ogólne składniki systemu (wymagania wstępne), które są niezbędne do zainstalowania aktualizacji. Na przykład, tymi wymaganiami wstępnymi mogą być aktualizacje systemu operacyjnego.

    Jeśli ta opcja jest wyłączona, konieczne może być ręczne zainstalowanie wymagań wstępnych.

    Domyślnie opcja ta jest wyłączona.

  - Tabela która wyświetla właściwości aktualizacji i zawierająca następujące kolumny:

    - **Nazwa**

      Nazwa aktualizacji.

    - **Opis**

      Opis aplikacji.

    - **Źródło**

      Źródło aktualizacji, czyli czy została ona wydana przez firmę Microsoft, czy przez inną niezależną firmę.

    - **Typ**

      Rodzaj aktualizacji, czyli czy jest przeznaczona dla sterownika czy aplikacji.

    - **Kategoria**

Kategoria Windows Server Update Services (WSUS) wyświetlana dla aktualizacji firmy Microsoft (aktualizacje krytyczne, aktualizacje definicji, sterowniki, pakiety funkcji, aktualizacje zabezpieczeń, dodatki Service Pack, narzędzia, pakiety zbiorcze aktualizacji, aktualizacje lub uaktualnienie).

- **Istotność zgodnie z MSRC**

  Istotność aktualizacji określona przez Microsoft Security Response Center (MSRC).

- **Istotność**

  Istotność aktualizacji określona przez Kaspersky.

- **Istotność poprawki (dla poprawek przeznaczonych dla aplikacji Kaspersky)**

  Istotność poprawki, jeśli jest ona przeznaczona dla aplikacji Kaspersky.

- **Artykuł**

  Identyfikator (ID) artykułu w bazie wiedzy opisującego aktualizację.

- **Biuletyn**

  Identyfikator biuletynu zabezpieczeń opisującego aktualizację.

- **Nieprzypisane do instalacji (nowa wersja)**

  Wyświetla, czy aktualizacja ma stan Nieprzypisane do instalacji.

- **Do zainstalowania**

  Wyświetla, czy aktualizacja ma stan Do zainstalowania.

- **Instalowanie**

  Wyświetla, czy aktualizacja ma stan Instalowanie.

- **Zainstalowano**

  Wyświetla, czy aktualizacja ma stan Zainstalowana.

- **Niepowodzenie**

  Wyświetla, czy aktualizacja ma stan Niepowodzenie.

- **Wymagane jest ponowne uruchomienie**

  Wyświetla, czy aktualizacja ma stan Wymagane ponowne uruchomienie.

- **Zarejestrowano**

  Wyświetla datę i godzinę rejestracji aktualizacji.

- **Zainstalowana w trybie interaktywnym**

  Wyświetla, czy aktualizacja wymaga interakcji z użytkownikiem podczas instalacji.

- **Wycofano**

  Wyświetla datę i godzinę odwołania aktualizacji.

- **Stan zatwierdzenia aktualizacji**

  Wyświetla, czy aktualizacja została zatwierdzona do instalacji.

- **Zmiana**

  Wyświetla aktualny numer wersji aktualizacji.

- **ID aktualizacji**

  Wyświetla identyfikator aktualizacji.

- **Wersja aplikacji**

  Wyświetla numer wersji, do której ma zostać zaktualizowana aplikacja.

- **Zastąpiony**

  Wyświetla inne aktualizacje, które mogą zastąpić aktualizację.

- **Zastępowanie**

  Wyświetla inne aktualizacje, które mogą zostać zastąpione przez aktualizację.

- **Akceptacja warunków Umowy licencyjnej jest wymagana**

  Wyświetla, czy aktualizacja wymaga akceptacji warunków Umowy licencyjnej(EULA).

- **Adres strony z opisem**

  Wyświetla nazwę producenta aktualizacji.

- **Rodzina aplikacji**

  Wyświetla nazwę rodziny aplikacji, do której należy aktualizacja.

- **Aplikacja**

Wyświetla nazwę aplikacji, do której należy aktualizacja.

- Wersja językowa

  Wyświetla język aktualizacji.

- Nieprzypisane do instalacji (nowa wersja)

  Wyświetla, czy aktualizacja ma stan Nie przypisano do instalacji (nowa wersja).

- Wymaga instalacji elementów należących do wymagań wstępnych

  Wyświetla, czy aktualizacja ma stan Wymaga instalacji wymagań wstępnych.

- Tryb pobierania

  Wyświetla tryb pobierania aktualizacji.

- Jest poprawką

  Wyświetla, czy aktualizacja jest poprawką.

- Nie zainstalowano

  Wyświetla, czy aktualizacja ma stan Nie zainstalowano.

- Tabela **Ustawienia**, która wyświetla ustawienia pakietu instalacyjnego — z ich nazwami, opisami i wartościami — użyte jako parametry wiersza poleceń podczas instalacji. Jeśli pakiet nie zawiera takich ustawień, wyświetlana jest odpowiednia wiadomość. Możesz zmodyfikować wartości tych ustawień.

- Zakładka **Historia rewizji** wyświetlająca rewizje pakietów instalacyjnych i zawierająca następujące kolumny:

  - Zmiana

    Wyświetla liczbę rewizji pakietów instalacyjnych.

  - Czas

    Wyświetla godzinę utworzenia rewizji.

  - Użytkownik

    Wyświetla nazwę konta użytkownika, pod którą została utworzona rewizja.

  - Akcja

    Wyświetla działanie (działania) wykonane na pakiecie instalacyjnym w obrębie rewizji.

  - Opis

Wyświetla opis tekstowy dodany do rewizji.

Znaczniki aplikacji

Ta sekcja opisuje znaczniki aplikacji oraz zawiera instrukcje ich tworzenia i modyfikowania oraz znakowania aplikacji firm trzecich.

Informacje o znacznikach aplikacji

Kaspersky Security Center umożliwia znakowanie aplikacji firm trzecich (aplikacje utworzone przez producentów oprogramowania innych niż firma Kaspersky). Znacznik to etykieta aplikacji, która może zostać użyta do grupowania lub wyszukiwania aplikacji. Znacznik przypisany do aplikacji może służyć jako warunek w wyborach urządzeń.

Na przykład, możesz utworzyć znacznik `[Browsers]` i przypisać go do wszystkich przeglądarek Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Tworzenie znacznika aplikacji

W celu utworzenia znacznika aplikacji:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Znaczniki aplikacji**.
2. Kliknij **Dodaj**.
   Zostanie otwarte okno nowego znacznika.
3. Wprowadź nazwę znacznika.
4. Kliknij **OK**, aby zachować zmiany.

Nowy znacznik pojawi się na liście znaczników aplikacji.

Zmienianie nazwy znacznika aplikacji

W celu zmiany nazwy znacznika aplikacji:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Znaczniki aplikacji**.
2. Zaznacz pole obok znacznika, którego nazwę chcesz zmienić, a następnie kliknij **Edytuj**.
   Zostanie otwarte okno właściwości znacznika.
3. Zmień nazwę znacznika.
4. Kliknij **OK**, aby zachować zmiany.

Zaktualizowany znacznik pojawi się na liście znaczników aplikacji.

Przydzielanie znaczników do aplikacji

W celu przydzielenia jednego lub kilku znaczników do aplikacji:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Rejestr aplikacji**.
2. Kliknij nazwę aplikacji, do której chcesz przydzielić znaczniki.
3. Wybierz zakładkę **Znaczniki**.

   Zakładka wyświetla wszystkie znaczniki aplikacji, które istnieją na Serwerze administracyjnym. Dla znaczników przypisanych do wybranej aplikacji, w kolumnie **Przypisany znacznik** zaznaczone jest pole.
4. Dla znaczników, które chcesz przypisać, w kolumnie **Przypisany znacznik** zaznacz pola.
5. Kliknij **Zapisz**, aby zachować zmiany.

Znaczniki zostają przypisane do aplikacji.

Usuwanie przydzielonych znaczników z aplikacji

W celu usunięcia jednego lub kilku znaczników z aplikacji:

1. W menu głównym przejdź do **Operacje → Aplikacje innych firm → Rejestr aplikacji**.
2. Kliknij nazwę aplikacji, z której chcesz usunąć znaczniki.
3. Wybierz zakładkę **Znaczniki**.

   Zakładka wyświetla wszystkie znaczniki aplikacji, które istnieją na Serwerze administracyjnym. Dla znaczników przypisanych do wybranej aplikacji, w kolumnie **Przypisany znacznik** zaznaczone jest pole.
4. Dla znaczników, które chcesz usunąć, w kolumnie **Przypisany znacznik** odznacz pola.
5. Kliknij **Zapisz**, aby zachować zmiany.

Znaczniki zostają usunięte z aplikacji.

Usunięte znaczniki aplikacji nie zostają całkowicie usunięte. Jeśli chcesz, możesz usunąć je ręcznie.

Usuwanie znacznika aplikacji

W celu usunięcia znacznika aplikacji:

1. W menu głównym przejdź do **Operacje** → **Aplikacje innych firm** → **Znaczniki aplikacji**.
2. Z listy wybierz znacznik aplikacji, który chcesz usunąć.
3. Kliknij przycisk **Usuń**.
4. W otwartym oknie potwierdzenia kliknij **OK**.

Znacznik aplikacji zostanie usunięty. Usunięty znacznik jest automatycznie usuwany ze wszystkich aplikacji, do których został przydzielony.

Monitorowanie i raportowanie

Ta sekcja opisuje możliwości monitorowania i raportowania Kaspersky Security Center. Te możliwości dają ogląd infrastruktury, stanów ochrony i statystyk.

Po zainstalowaniu programu Kaspersky Security Center lub podczas jego działania, możesz skonfigurować funkcje monitorowania i raportowania, aby najlepiej odpowiadały Twoim potrzebom.

Scenariusz: Monitorowanie i raportowanie

Ta sekcja zawiera scenariusz konfigurowania funkcji monitorowania i raportowania w Kaspersky Security Center.

Wymagania wstępne

Po wdrożeniu Kaspersky Security Center w sieci organizacji, możesz uruchomić jej monitorowanie i wygenerować raporty dotyczące jej funkcjonowania.

Monitorowanie i raportowanie w sieci organizacji odbywa się w etapach:

1. **Konfigurowanie przełączania stanów urządzeń**

   Zapoznaj się z ustawieniami stanów urządzeń w zależności od określonych warunków. Zmieniając te ustawienia, możesz zmienić liczbę zdarzeń z priorytetami *Krytyczne* lub *Ostrzeżenie*. Podczas konfigurowania przełączania stanów urządzeń, upewnij się, że:

   - Nowe ustawienia nie są sprzeczne z polityką bezpieczeństwa informacji, obowiązującą w Twojej firmie.
   - Możesz reagować na ważne zdarzenia dotyczące bezpieczeństwa w sieci Twojej organizacji w odpowiednim momencie.

2. **Konfigurowanie powiadomień o zdarzeniach występujących na urządzeniach klienckich**

   Dostępne instrukcje:

   Skonfiguruj powiadamianie (poprzez e-mail, wiadomość SMS lub przez uruchomienie pliku wykonywalnego) o zdarzeniach na urządzeniach klienckich

3. **Zmiana reakcji ochrony sieci na zdarzenie Epidemia wirusa**

Możesz zmienić określone wartości progowe we właściwościach Serwera administracyjnego. Możesz także utworzyć rygorystyczną zasadę, która zostanie aktywowana, lub utworzyć zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.

4. **Wykonywanie zalecanych działań dla powiadomień krytycznych i ostrzegających**

   Dostępne instrukcje:

   Wykonaj zalecane działania dla sieci w swojej organizacji

5. **Sprawdzanie stanu ochrony sieci w swojej organizacji**

   Dostępne instrukcje:

   - Sprawdź widżeta Stan ochrony
   - Wygeneruj i sprawdź Raport o stanie ochrony
   - Wygeneruj i przeczytaj Raport o błędach

6. **Lokalizowanie urządzeń klienckich, które nie są chronione**

   Dostępne instrukcje:

   - Przejrzyj widżet Nowe urządzenia
   - Wygeneruj i przeczytaj Raport wdrażania ochrony

7. **Sprawdzanie ochrony urządzeń klienckich**

   Dostępne instrukcje:

   - Wygeneruj i sprawdź raporty z kategorii Stan ochrony i Statystyki zagrożeń
   - Uruchom i sprawdź wybór zdarzeń Krytyczny

8. **Oszacowanie i ograniczenie nagromadzenia zdarzeń w bazie danych**

   Informacje o zdarzeniach występujących podczas działania zarządzanych aplikacji są przesyłane z urządzenia klienckiego i zapisywane w bazie danych Serwera administracyjnego. Aby zmniejszyć obciążenie na Serwerze administracyjnym, oszacuj i ogranicz maksymalną liczbę zdarzeń przechowywanych w bazie danych.

   Dostępne instrukcje:

   - Obliczanie pojemności bazy danych
   - Ograniczanie maksymalnej liczby zdarzeń

9. **Przeglądanie informacji o licencji**

   Dostępne instrukcje:

   - Dodaj widżet Użycie kluczy licencyjnych do pulpitu nawigacyjnego i sprawdź go
   - Wygeneruj i przeczytaj Raport o użyciu kluczy licencyjnych

Wyniki

Po zakończeniu scenariusza zostaniesz poinformowany o ochronie sieci w swojej organizacji i tym samym będziesz mógł zaplanować działania związane z dalszą ochroną.

Informacje o typach monitorowania i raportowania

Informacje na temat zdarzeń dotyczących bezpieczeństwa w sieci organizacji są przechowywane w bazie danych Serwera administracyjnego. Na podstawie zdarzeń Kaspersky Security Center Web Console oferuje następujące typy monitorowania i raportowania w sieci Twojej organizacji:

- Pulpit nawigacyjny
- Raporty
- Wybory zdarzeń
- Powiadomienia

Pulpit nawigacyjny

Pulpit nawigacyjny umożliwia monitorowanie trendów bezpieczeństwa w sieci Twojej organizacji poprzez graficzne przedstawienie informacji.

Raporty

Raporty umożliwiają uzyskanie szczegółowych informacji liczbowych na temat ochrony sieci Twojej organizacji, zapisania tych informacji w pliku, wysłania ich w wiadomości e-mail oraz ich wydrukowania.

Wybory zdarzeń

Wybory zdarzeń oferują widok ekranowy nazwanych zestawów zdarzeń, które są wybrane z bazy danych Serwera administracyjnego. Te zestawy zdarzeń są grupowane zgodnie z następującymi kategoriami:

- Według istotności—**Zdarzenia krytyczne**, **Błędy funkcjonalne**, **Ostrzeżenia** i **Informacja o zdarzeniach**
- Według czasu—**Ostatnie zdarzenia**
- Według typu—**Żądania użytkownika** and **Zdarzenia audytu**

Możesz tworzyć i przeglądać wybory zdarzeń zdefiniowane przez użytkownika oparte na ustawieniach dostępnych do konfiguracji w interfejsie Kaspersky Security Center Web Console.

Powiadomienia

Powiadomienia informują o zdarzeniach oraz pomagają w przyspieszeniu odpowiedzi na te zdarzenia poprzez wykonanie zalecanych działań lub działań, które uznajesz za odpowiednie.

Pulpit nawigacyjny i widżety

Ta sekcja zawiera informacje o panelu kontrolnym i widżetach udostępnianych przez panel kontrolny. Sekcja zawiera instrukcje dotyczące zarządzania widżetami i konfigurowania ich ustawień.

Korzystanie z pulpitu nawigacyjnego

Pulpit nawigacyjny umożliwia monitorowanie trendów bezpieczeństwa w sieci Twojej organizacji poprzez graficzne przedstawienie informacji.

Pulpit nawigacyjny jest dostępny w Kaspersky Security Center Web Console w sekcji **Monitorowanie i raportowanie** po kliknięciu **Pulpit nawigacyjny**.

Pulpit nawigacyjny zawiera widżety, które można dostosować. Możesz wybrać dużą liczbę różnych widżetów, przedstawionych w postaci wykresu kołowego lub diagramu pierścieniowego, tabeli, wykresów, wykresów słupkowych oraz list. Informacje wyświetlane w widżetach są automatycznie aktualizowane, okres aktualizacji wynosi od jednej do dwóch minut. Przedział czasu między aktualizacjami jest inny dla każdego widżeta. Możesz ręcznie odświeżyć dane dotyczące widżeta w dowolnym momencie, korzystając z menu ustawień.

Domyślnie widżety zawierają informacje o wszystkich zdarzeniach przechowywanych w bazie danych Serwera administracyjnego.

Kaspersky Security Center Web Console zawiera domyślny zestaw widżetów należących do następujących kategorii:

- **Stan ochrony**
- **Wdrażanie**
- **Aktualizowanie**
- **Statystyki zagrożeń**
- **Inne**

Niektóre widżety posiadają informacje tekstowe z odnośnikami. Po kliknięciu odnośnika zostaną wyświetlone informacje szczegółowe.

Podczas konfigurowania pulpitu nawigacyjnego możesz dodać widżety, których potrzebujesz, ukryć widżety, których nie potrzebujesz, zmienić rozmiar lub wygląd widżetów, przenieść widżety, a także zmienić ich ustawienia.

Dodawanie widżetów do pulpitu nawigacyjnego

W celu dodania widżetów do pulpitu nawigacyjnego:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij przycisk **Dodaj lub przywróć widżet sieciowy**.
3. Na liście dostępnych widżetów wybierz widżety, które chcesz dodać do pulpitu nawigacyjnego.

   Widżety są pogrupowane według kategorii. Aby wyświetlić listę widżetów należących do kategorii, kliknij ikonę strzałki skierowanej w prawo (>), znajdującą się obok nazwy kategorii.
4. Kliknij przycisk **Dodaj**.

Wybrane widżety zostaną dodane na końcu pulpitu nawigacyjnego.

Teraz możesz edytować reprezentację i parametry dodanych widżetów.

Ukrywanie widżetu na pulpicie nawigacyjnym

W celu ukrycia widżetu na pulpicie nawigacyjnym:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia(⚙), znajdującą się obok widżetu, który chcesz ukryć.
3. Wybierz **Ukryj widżet sieciowy**.
4. W otwartym oknie **Ostrzeżenie** kliknij **OK**.

Wybrany widżet zostanie ukryty. Następnie możesz ponownie dodać ten widżet do pulpitu nawigacyjnego.

Przenoszenie widżetu na pulpicie nawigacyjnym

W celu przeniesienia widżetu na pulpicie nawigacyjnym:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz przenieść.
3. Wybierz **Przenieś**.
4. Kliknij miejsce, do którego chcesz przenieść widżet. Możesz wybrać tylko inny widżet.

Miejsca wybranych widżetów zostaną zamienione.

Zmiana wyglądu i rozmiaru widżetu

Dla widżetów, które wyświetlają wykres, możesz zmienić jego reprezentację-wykres słupkowy lub wykres liniowy. Dla niektórych widżetów możesz zmienić ich rozmiar: kompaktowy, średni lub maksymalny.

W celu zmiany reprezentacji widżetu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz edytować.
3. Wykonaj jedną z poniższych czynności:
   - Aby wyświetlić widżet jako wykres słupkowy, wybierz **Typ wykresu: Słupki**.
   - Aby wyświetlić widżet jako wykres liniowy, wybierz **Typ wykresu: Linie**.

- W celu zmiany obszaru zajętego przez widżet, wybierz jedną z wartości:
  - **Kompaktowy**
  - **Kompaktowy (tylko słupek)**
  - **Średni (wykres pierścieniowy)**
  - **Średni (wykres słupkowy)**
  - **Maksymalny**

Reprezentacja wybranego widżetu zostanie zmieniona.

Zmiana ustawień widżetu

W celu zmiany ustawień widżetu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Pulpit nawigacyjny**.
2. Kliknij ikonę ustawienia (⚙), znajdującą się obok widżetu, który chcesz zmienić.
3. Wybierz **Pokaż ustawienia**.
4. Jeśli zostanie otwarte okno ustawień widżetu, zmień ustawienia widżetu zgodnie z wymaganiami.
5. Kliknij **Zapisz**, aby zachować zmiany.

Ustawienia wybranego widżetu zostaną zmienione.

Zestaw ustawień zależy od określonego widżetu. Poniżej znajdują się podstawowe ustawienia:

- **Obszar widżetu webowego** (zestaw obiektów, dla których widżet wyświetla informacje)—na przykład, grupa administracyjna lub wybór urządzeń.
- **Wybierz zadanie** (zadanie, dla którego widżet wyświetla informacje).
- **Przedział czasu** (przedział czasu, w trakcie którego informacje są wyświetlane w widżecie)—między dwoma określonymi datami; od określonej daty do bieżącego dnia; lub od bieżącego dnia minus określoną liczbę dni do bieżącego dnia.
- **Ustaw stan Krytyczny, jeśli** i **Ustaw stan Ostrzeżenie, jeśli** (reguły, które określają kolor wskaźnika).

Informacje o trybie samego pulpitu

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

Gdy użytkownik pracuje w trybie samego pulpitu, stosowane są następujące ograniczenia:

- Menu główne nie jest wyświetlane użytkownikowi, więc nie może on zmienić ustawień ochrony sieci.
- Użytkownik nie może wykonywać żadnych akcji z widżetami, na przykład dodawać widżetów lub ich ukrywać. Dlatego należy umieścić w pulpicie nawigacyjnym wszystkie potrzebne użytkownikowi widżety i skonfigurować je, np. ustawić zasadę liczenia obiektów lub określić przedział czasowy.

Nie można przypisać sobie trybu samego pulpitu. Jeśli chcesz pracować w tym trybie, skontaktuj się z administratorem systemu, dostawcą usług zarządzanych (MSP) lub użytkownikiem z uprawnieniami **Modyfikacja listy ACL obiektów** w obszarze **Funkcje ogólne: uprawnienia użytkownika**.

Konfigurowanie trybu samego pulpitu

Zanim zaczniesz konfigurować tryb samego pulpitu, upewnij się, że spełnione są następujące wymagania wstępne:

- Masz uprawnienia **Modyfikacja list ACL obiektów** w obszarze funkcjonalnym **Funkcje ogólne: uprawnienia użytkownika**. Jeśli nie masz tych uprawnień, nie będzie zakładki do konfiguracji trybu.
- Użytkownik ma uprawnienia **Odczyt** w obszarze funkcjonalnym **Funkcje ogólne: funkcjonalność podstawowa**.

Jeśli w Twojej sieci istnieje hierarchia Serwerów administracyjnych, aby skonfigurować tryb samego pulpitu, przejdź do serwera, na którym dostępne jest konto użytkownika w sekcji **Użytkownicy i role → Użytkownicy**. Może to być serwer główny lub fizyczny serwer pomocniczy. Nie ma możliwości dostosowania trybu na serwerze wirtualnym.

W celu skonfigurowania trybu samego pulpitu:

1. W menu głównym przejdź do **Użytkownicy i role → Użytkownicy**.
2. Kliknij nazwę konta użytkownika, dla którego chcesz dostosować pulpit nawigacyjny za pomocą widżetów.
3. W otwartym oknie ustawień konta wybierz zakładkę **Pulpit nawigacyjny**.

   Na karcie, która się otworzy, zostanie wyświetlony ten sam pulpit nawigacyjny, co pulpit dla użytkownika.
4. Jeśli opcja **Wyświetlaj konsolę tylko w trybie samego pulpitu** jest włączona, przełącz przełącznik, aby ją wyłączyć.

   Gdy ta opcja jest włączona, nie można również zmienić pulpitu nawigacyjnego. Po wyłączeniu opcji możesz zarządzać widżetami.
5. Skonfiguruj wygląd pulpitu nawigacyjnego. Zestaw widżetów przygotowany w zakładce **Pulpit nawigacyjny** jest dostępny dla użytkownika z konfigurowalnym kontem. Użytkownik nie może zmieniać żadnych ustawień ani rozmiaru widżetów, dodawać ani usuwać żadnych widżetów z pulpitu nawigacyjnego. Dlatego dostosuj je dla użytkownika, aby mógł przeglądać statystyki ochrony sieci. W tym celu w zakładce **Pulpit nawigacyjny** możesz wykonać te same akcje z widżetami, co w sekcji **Monitorowanie i raportowanie → Pulpit nawigacyjny**:
   - Dodaj nowe widżety do pulpitu nawigacyjnego.
   - Ukryj widżety, których użytkownik nie potrzebuje.
   - Przenieś widżety w określonej kolejności.

- Zmień rozmiar lub wygląd widżetów.
- Zmień ustawienia widżetu.

6. Przełącz przycisk przełącznika, aby włączyć opcję **Wyświetlaj konsolę w trybie samego pulpitu**.

   Następnie dla użytkownika dostępny będzie tylko pulpit nawigacyjny. Użytkownik może monitorować statystyki, ale nie może zmieniać ustawień ochrony sieci i wyglądu pulpitu nawigacyjnego. Ponieważ wyświetlany jest ten sam pulpit nawigacyjny, co dla użytkownika, nie można również zmienić pulpitu nawigacyjnego.

   Jeśli pozostawisz tę opcję wyłączoną, dla użytkownika zostanie wyświetlone menu główne, dzięki czemu będzie on mógł wykonywać różne akcje w Kaspersky Security Center, w tym zmieniać ustawienia bezpieczeństwa i widżety.

7. Po zakończeniu konfigurowania trybu samego pulpitu kliknij przycisk **Zapisz**. Dopiero po tym przygotowany pulpit nawigacyjny zostanie wyświetlony użytkownikowi.

8. Jeśli użytkownik chce przeglądać statystyki obsługiwanych aplikacji Kaspersky i potrzebuje do tego uprawnień dostępu, skonfiguruj uprawnienia dla użytkownika. Następnie dane aplikacji Kaspersky będą wyświetlane dla użytkownika w widżetach tych aplikacji.

Teraz użytkownik może zalogować się do Kaspersky Security Center na swoim koncie i monitorować statystyki ochrony sieci w trybie samego pulpitu.

Raporty

W tej sekcji opisano, jak używać raportów, zarządzać niestandardowymi szablonami raportów, używać szablonów raportów do generowania nowych raportów i tworzyć zadania dostarczania raportów.

Korzystanie z raportów

Raporty umożliwiają uzyskanie szczegółowych informacji liczbowych na temat ochrony sieci Twojej organizacji, zapisania tych informacji w pliku, wysłania ich w wiadomości e-mail oraz ich wydrukowania.

Raporty są dostępne w Kaspersky Security Center Web Console w sekcji **Monitorowanie i raportowanie** po kliknięciu **Raporty**.

Domyślnie, raporty zawierają informacje dla ostatnich 30 dni.

Kaspersky Security Center posiada domyślny zestaw raportów należących do następujących kategorii:

- **Stan ochrony**
- **Wdrażanie**
- **Aktualizowanie**
- **Statystyki zagrożeń**
- **Inne**

Możesz tworzyć niestandardowe szablony raportu, edytować szablony raportu oraz usuwać je.

Możesz tworzyć raporty, które są oparte na istniejących szablonach, eksportować raporty do plików, a także tworzyć zadania dostarczania raportów.

Tworzenie szablonu raportu

W celu utworzenia szablonu raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
3. W pierwszym kroku kreatora wprowadź nazwę raportu i wybierz typ raportu.
4. W kroku **Zakres** wybierz zestaw urządzeń klienckich (grupę administracyjną, wybór urządzeń, wybrane urządzenia lub wszystkie urządzenia w sieci), których dane zostaną wyświetlone w raportach, które są oparte na tym szablonie raportu.
5. Na stronie **Okres raportowania** kreatora określ okres raportowania. Dostępne wartości wyglądają następująco:

   - Między dwoma określonymi datami
   - Od określonej daty do daty utworzenia raportu
   - Od daty utworzenia raportu minus określona liczba dni do daty utworzenia raportu

   Dla niektórych raportów ta strona może nie być wyświetlana.
6. Kliknij **OK**, aby zamknąć kreator.
7. Wykonaj jedną z poniższych czynności:

   - Kliknij przycisk **Zapisz i uruchom**, aby zapisać nowy szablon raportu i uruchomić raport w oparciu o niego.

     Szablon raportu zostanie zapisany. Raport zostanie wygenerowany.
   - Kliknij przycisk **Zapisz**, aby zapisać nowy szablon raportu.

     Szablon raportu zostanie zapisany.

Możesz użyć nowego szablonu do generowania i wyświetlania raportów.

Przeglądanie i edytowanie właściwości szablonu raportu

Możesz przeglądać i edytować podstawowe właściwości szablonu raportu, na przykład, nazwę szablonu raportu lub pola wyświetlane w raporcie.

W celu przejrzenia i edytowania właściwości szablonu raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.

2. Zaznacz pole obok szablonu raportu, którego właściwości chcesz przejrzeć i edytować.

   Alternatywnie możesz w pierwszej kolejności wygenerować raport, a następnie kliknąć przycisk **Edytuj**.

3. Kliknij przycisk **Otwórz właściwości szablonu raportu**.

   Zostanie otwarte okno **Edytowanie raportu <Nazwa raportu>** na zakładce **Ogólne**.

4. Edytuj właściwości szablonu raportu:

   - Zakładka **Ogólne**:

     - Nazwa szablonu raportu

     - **Maksymalna liczba wyświetlanych wpisów**

       Jeśli ta opcja jest włączona, liczba wpisów wyświetlanych w tabeli ze szczegółowymi danymi raportu nie wynosi więcej niż określona wartość.

       Wpisy w raporcie są najpierw przechowywane zgodnie z regułami określonymi w sekcji **Pola → Pola szczegółów** właściwości szablonu raportu, a następnie przechowywane są tylko pierwsze wpisy wynikowe. Nagłówek tabeli ze szczegółowymi danymi raportu pokazuje wyświetloną liczbę wpisów oraz całkowitą dostępną liczbę wpisów, które odpowiadają ustawieniom innego szablonu raportu.

       Jeśli ta opcja jest wyłączona, tabela ze szczegółowymi danymi raportu wyświetla wszystkie dostępne wpisy. Nie jest zalecane wyłączenie tej opcji. Ograniczenie liczby wyświetlanych wpisów raportu zmniejsza obciążenie systemu zarządzania bazą danych (DBMS) i skraca czas wymagany do wygenerowania i eksportowania raportu. Niektóre z raportów zawierają zbyt wiele wpisów. W takiej sytuacji może być trudno przeczytać i przeanalizować je wszystkie. Dodatkowo, podczas tworzenia takiego raportu, na Twoim urządzeniu może zabraknąć pamięci, co w konsekwencji uniemożliwi przejrzenie raportu.

       Domyślnie opcja ta jest włączona. Domyślna wartość to 1000.

     - **Grupa**

       Kliknij przycisk **Ustawienia**, aby zmienić zestaw urządzeń klienckich, dla których tworzony jest raport. Dla niektórych typów raportów przycisk może być niedostępny. Rzeczywiste ustawienia zależą od ustawień określonych podczas tworzenia szablonu raportu.

     - **Przedział czasu**

       Kliknij przycisk **Ustawienia**, aby zmodyfikować okres raportowania. Dla niektórych typów raportów przycisk może być niedostępny. Dostępne wartości wyglądają następująco:

       - Między dwoma określonymi datami
       - Od określonej daty do daty utworzenia raportu
       - Od daty utworzenia raportu minus określona liczba dni do daty utworzenia raportu

     - **Dołącz dane z podrzędnych i wirtualnych Serwerów administracyjnych**

       Jeśli ta opcja jest włączona, raport zawiera informacje z podrzędnych i wirtualnych Serwerów administracyjnych, które podlegają Serwerowi administracyjnemu, dla którego utworzono szablon raportu.

       Wyłącz tę opcję, jeśli chcesz przejrzeć dane tylko z bieżącego Serwera administracyjnego.

       Domyślnie opcja ta jest włączona.

- **Do poziomu zagnieżdżenia**

  Raport zawiera dane z podrzędnych i wirtualnych Serwerów administracyjnych, które znajdują się pod bieżącym Serwerem administracyjnym na poziomie zagnieżdżenia, który jest mniejszy niż lub równy określonej wartości.

  Domyślna wartość to 1. Możesz chcieć zmienić tę wartość, jeśli musisz zbierać informacje z podrzędnych Serwerów administracyjnych znajdujących się na niższych poziomach drzewa.

- **Czas oczekiwania na dane (min)**

  Przed wygenerowaniem raportu, Serwer administracyjny, dla którego tworzony jest szablon raportu, oczekuje na dane z podrzędnych Serwerów administracyjnych przez określoną liczbę minut. Jeśli żadne dane nie są pobierane z podrzędnego Serwera administracyjnego pod koniec tego okresu, raport i tak zostanie uruchomiony. Zamiast rzeczywistych danych, raport wyświetla dane pobrane z pamięci podręcznej (jeśli opcja **Buforuj dane z podrzędnych Serwerów administracyjnych** jest włączona) lub **N/A** (nie jest dostępne) w innym przypadku.

  Domyślna wartość to 5 (minuty).

- **Buforuj dane z podrzędnych Serwerów administracyjnych**

  Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Przesłane dane są przechowywane w pamięci podręcznej.

  Jeśli podczas generowania raportu bieżący Serwer administracyjny nie może odbierać danych z podrzędnego Serwera administracyjnego, raport wyświetla dane pobrane z pamięci podręcznej. Wyświetlana jest także data przesłania danych do pamięci podręcznej.

  Włączenie tej opcji umożliwia przeglądanie informacji z podrzędnych Serwerów administracyjnych nawet wtedy, gdy aktualne dane nie mogą zostać pobrane. Jednakże wyświetlane dane mogą być przestarzałe.

  Domyślnie opcja ta jest wyłączona.

- **Częstotliwość aktualizacji pamięci podręcznej (godz.)**

  Podrzędne Serwery administracyjne regularnie przesyłają dane do Serwera administracyjnego, dla którego został utworzony szablon raportu. Możesz określić ten okres w godzinach. Jeśli określisz 0 godzin, dane są przesyłane tylko wtedy, gdy raport zostaje wygenerowany.

  Domyślna wartość to 0.

- **Prześlij szczegółowe informacje z podrzędnych Serwerów administracyjnych**

  W wygenerowanym raporcie tabela ze szczegółowymi danymi raportu zawiera dane z podrzędnych Serwerów administracyjnych Serwera administracyjnego, dla którego został utworzony szablon raportu.

  Włączenie tej opcji spowalnia tworzenie raportu i zwiększa ruch sieciowy między Serwerami administracyjnymi. Jednakże możesz przejrzeć wszystkie dane w jednym raporcie.

  Zamiast włączyć tę opcję, możesz chcieć przeanalizować szczegółowe dane raportu, aby wykryć wadliwy podrzędny Serwer administracyjny, a następnie wygenerować ten sam raport tylko dla tego wadliwego Serwera administracyjnego.

  Domyślnie opcja ta jest wyłączona.

- Zakładka **Pola**

  Wybierz pola, które będą wyświetlane w raporcie i użyj przycisku **W górę** oraz przycisku **W dół**, aby zmienić kolejność tych pól. Użyj przycisku **Dodaj** lub przycisku **Edytuj**, aby określić, czy informacje w raporcie muszą być sortowane i filtrowane według każdego z pól.

  W sekcji **Pola filtrów szczegółów** możesz również kliknąć przycisk **Konwertuj filtry**, aby rozpocząć korzystanie z rozszerzonego formatu filtrowania. Ten format umożliwia łączenie warunków filtrowania określonych w różnych polach za pomocą operacji logicznej LUB. Po kliknięciu przycisku po prawej stronie zostanie otwarty panel **Konwertuj filtry**. Kliknij przycisk **Konwertuj filtry**, aby potwierdzić konwersję. Możesz teraz zdefiniować przekonwertowany filtr z warunkami z sekcji **Pola szczegółów**, które są stosowane przy użyciu operacji logicznej LUB.

  > Konwersja raportu do formatu obsługującego złożone warunki filtrowania spowoduje, że raport będzie niezgodny z poprzednimi wersjami Kaspersky Security Center (11 i starszymi). Przekonwertowany raport nie będzie zawierał żadnych danych z podrzędnych Serwerów administracyjnych, na których działają takie niekompatybilne wersje.

5. Kliknij **Zapisz**, aby zachować zmiany.

6. Zamknij okno **Edycja raportu <Nazwa raportu>**.

Zaktualizowany szablon raportu pojawi się na liście szablonów raportu.

Eksportowanie raportu do pliku

Możesz wyeksportować raport do pliku XML, HTML lub PDF.

W celu wyeksportowania raportu do pliku:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.

2. Zaznacz pole obok raportu, który chcesz wyeksportować do pliku.

3. Kliknij przycisk **Eksportuj raport**.

4. W otwartym oknie, w polu **Nazwa** zmień nazwę pliku raportu. Domyślnie, nazwa pliku pokrywa się z nazwą wybranego szablonu raportu.

5. Wybierz typ pliku raportu: XML, HTML lub PDF.

6. Kliknij przycisk **Eksportuj raport**.

   Raport w wybranym formacie zostanie pobrany na Twoje urządzenie—do folderu domyślnego Twojego urządzenia—lub zostanie otwarte standardowe okno **Zapisywanie jako** w Twojej przeglądarce, aby umożliwić Ci zapisanie pliku w miejscu, w którym chcesz.

Raport zostanie zapisany do pliku.

Generowanie i przeglądanie raportu

W celu utworzenia i przejrzenia raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.
2. Kliknij nazwę szablonu raportu, którego chcesz użyć do utworzenia raportu.

Raport zostanie wygenerowany przy użyciu wybranego szablonu i wyświetlony.

Dane raportu są wyświetlane zgodnie z lokalizacją ustawioną dla Serwera administracyjnego.

Raport wyświetla następujące dane:

- Na zakładce **Podsumowanie**:
  - Nazwę i typ raportu, krótki opis i okres raportowania, a także informacje o grupie urządzeń, dla których generowany jest raport.
  - Wykres graficzny przedstawiający najbardziej reprezentatywne dane raportu.
  - Tabelę zbiorczą z wyliczonymi wskaźnikami raportu.
- Na zakładce **Szczegóły** wyświetlona zostanie tabela ze szczegółowymi danymi raportu.

Tworzenie zadania dostarczania raportu

Możesz utworzyć zadanie, które będzie dostarczać wybrane raporty.

W celu utworzenia zadania dostarczania raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.
2. [Opcjonalnie] Zaznacz pole obok szablonów raportu, dla którego chcesz utworzyć zadanie dostarczania raportu.
3. Kliknij przycisk **Nowe zadanie dostarczania raportu**.
4. Zostanie uruchomiony Kreator tworzenia nowego zadania. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
5. W pierwszym kroku kreatora wprowadź nazwę zadania. Domyślna nazwa to **Dostarcz raporty (<N>)**, gdzie <N> to numer seryjny zadania.
6. W kroku ustawień zadania określ następujące ustawienia:
   a. Szablony raportu, które zostaną dostarczone przez zadanie. Jeśli wybrałeś je w kroku 2, pomiń ten krok.
   b. Format raportu: HTML, XLS lub PDF.
   c. Czy raporty są wysyłane za pośrednictwem poczty elektronicznej wraz z ustawieniami powiadomień e-mail.
   d. Czy raporty są zapisywane do folderu, czy wcześniej zapisane raporty w tym folderze są nadpisywane i czy określone konto będzie używane do uzyskania dostępu do tego folderu (dla folderu współdzielonego).

7. Jeśli chcesz zmodyfikować inne ustawienia zadania po utworzeniu zadania, na stronie **Zakończ tworzenie zadania** kreatora włącz opcję **Otwórz szczegóły zadania po jego utworzeniu**.

8. Kliknij przycisk **Utwórz**, aby utworzyć zadanie i zamknąć kreator.

   Zostanie utworzone zadanie dostarczania raportów. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, zostanie otwarte okno ustawień zadania.

Usuwanie szablonów raportu

W celu usunięcia jednego lub kilku szablonów raportu:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Raporty**.

2. Zaznacz pola obok szablonów raportu, które chcesz usunąć.

3. Kliknij przycisk **Usuń**.

4. W otwartym oknie kliknij **OK**, aby potwierdzić swój wybór.

Wybrane szablony raportu zostaną usunięte. Jeśli te szablony raportu znajdowały się w zadaniach dostarczania raportów, zostaną usunięte z zadań.

Zdarzenia i wybory zdarzeń

Ta sekcja zawiera informacje o zdarzeniach i wyborach zdarzeń, o typach zdarzeń występujących w komponentach Kaspersky Security Center oraz o zarządzaniu blokowaniem częstych zdarzeń.

Używanie wyborów zdarzeń

Wybory zdarzeń oferują widok ekranowy nazwanych zestawów zdarzeń, które są wybrane z bazy danych Serwera administracyjnego. Te zestawy zdarzeń są grupowane zgodnie z następującymi kategoriami:

- Według istotności—**Zdarzenia krytyczne**, **Błędy funkcjonalne**, **Ostrzeżenia** i **Informacja o zdarzeniach**
- Według czasu—**Ostatnie zdarzenia**
- Według typu—**Żądania użytkownika** and **Zdarzenia audytu**

Możesz tworzyć i przeglądać wybory zdarzeń zdefiniowane przez użytkownika oparte na ustawieniach dostępnych do konfiguracji w interfejsie Kaspersky Security Center Web Console.

Wybory zdarzeń są dostępne w Kaspersky Security Center Web Console w sekcji **Monitorowanie i raportowanie** po kliknięciu **Wybory zdarzeń**.

Domyślnie, wybory zdarzeń zawierają informacje dla ostatnich siedmiu dni.

Kaspersky Security Center posiada domyślny (predefiniowany) zestaw wyborów zdarzeń:

- Zdarzenia z różnymi priorytetami:
  - **Zdarzenia krytyczne**
  - **Błędy funkcjonalne**
  - **Ostrzeżenia**
  - **Zdarzenie informacyjne**
- **Żądania użytkownika** (zdarzenia zarządzanych aplikacji)
- **Ostatnie zdarzenia** (w ostatnim tygodniu)
- **Zdarzenia audytu**.

Możesz także utworzyć i skonfigurować dodatkowe wybory zdefiniowane przez użytkownika. W wyborach zdefiniowanych przez użytkownika możesz filtrować zdarzenia według właściwości urządzeń, z których pochodzą (nazwy urządzeń, zakresy IP i grupy administracyjne), według typów zdarzeń i priorytetów, według aplikacji i nazwy komponentu oraz według przedziału czasu. Możliwe jest także uwzględnienie wyników zadania w obszarze wyszukiwania. Możesz także użyć pola prostego wyszukiwania, gdzie można wpisać słowo lub kilka słów. Zostaną wyświetlone wszystkie zdarzenia, które zawierają dowolne z wpisanych słów w swoich atrybutach (takie jak: nazwa zdarzenia, opis, nazwa komponentu).

Dla predefiniowanych wyborów oraz wyborów zdefiniowanych przez użytkownika możesz ograniczyć liczbę wyświetlanych zdarzeń lub liczbę wyszukiwanych wpisów. Obie opcje wpływają na czas, jakie zajmuje programowi Kaspersky Security Center wyświetlanie zdarzeń. Im większa baza danych, tym więcej czasu może zająć proces.

Możesz wykonać następujące czynności:

- Edytuj właściwości wyborów zdarzeń
- Wygeneruj wybory zdarzeń
- Zobacz szczegóły wyborów zdarzeń
- Usuń wybory zdarzeń
- Usuń zdarzenia z bazy danych Serwera administracyjnego

Tworzenie kryterium wyboru zdarzenia

W celu utworzenia wyboru zdarzeń:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Wybory zdarzeń**.
2. Kliknij **Dodaj**.
3. W otwartym oknie **Nowy wybór zdarzeń** określ ustawienia nowego wyboru zdarzeń. Wykonaj te czynności w jednej lub kilku sekcjach w oknie.
4. Kliknij **Zapisz**, aby zachować zmiany.

   Zostanie otwarte okno potwierdzenia.

5. Aby sprawdzić wynik wyboru zdarzenia, pozostaw pole **Przejdź do wyniku wyboru** zaznaczone.

6. Kliknij **Zapisz**, aby potwierdzić tworzenie wyboru zdarzenia.

Jeśli pozostawiłeś pole **Przejdź do wyniku wyboru** zaznaczone, zostanie wyświetlony wynik wyboru zdarzenia. Jeśli tak się nie stanie, nowy wybór zdarzenia pojawi się na liście wyborów zdarzeń.

Edytowanie kryterium wyboru zdarzenia

W celu edytowania kryterium wyboru zdarzenia:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Wybory zdarzeń**.

2. Zaznacz pole obok wyboru zdarzeń, który chcesz edytować.

3. Kliknij przycisk **Właściwości**.

   Zostanie otwarte okno ustawień wyboru zdarzenia.

4. Edytuj właściwości wyboru zdarzenia.

   > Dla predefiniowanych wyborów zdarzeń możesz edytować tylko właściwości na następujących zakładkach: **Ogólne** (za wyjątkiem nazwy wyboru), **Czas** i **Prawa dostępu**.

   Dla wyborów zdefiniowanych przez użytkownika możesz edytować wszystkie właściwości.

5. Kliknij **Zapisz**, aby zachować zmiany.

Edytowany wybór zdarzenia zostanie wyświetlony na liście.

Przeglądanie listy wyboru zdarzeń

W celu przejrzenia wyboru zdarzeń:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Wybory zdarzeń**.

2. Zaznacz pole obok wyboru zdarzeń, który chcesz uruchomić.

3. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz skonfigurować sortowanie w wyniku wyboru zdarzeń, wykonaj następujące czynności:

     a. Kliknij przycisk **Skonfiguruj sortowanie i uruchom**.

     b. W wyświetlonym oknie **Skonfiguruj sortowanie wyboru zdarzeń** określ ustawienia sortowania.

     c. Kliknij nazwę wyboru.

- W innej sytuacji, jeśli chcesz przejrzeć listę zdarzeń posortowanych na Serwerze administracyjnym, kliknij nazwę wyboru.

Zostanie wyświetlony wynik wyboru zdarzeń.

Przeglądanie szczegółów zdarzenia

W celu przejrzenia szczegółów zdarzenia:

1. Uruchom wybór zdarzeń.
2. Kliknij czas żądanego zdarzenia.
   Zostanie otwarte okno **Właściwości zdarzenia**.
3. W wyświetlonym oknie możesz wykonać następujące czynności:
   - Przejrzeć informacje o wybranym zdarzeniu
   - Przejść do kolejnych i poprzednich zdarzeń w wyniku wyboru zdarzeń
   - Przejść do urządzenia, na którym wystąpiło zdarzenie
   - Przejść do grupy administracyjnej, która zawiera urządzenie, na którym wystąpiło zdarzenie
   - W przypadku zdarzenia związanego z zadaniem przejdź do właściwości zadania

Eksportowanie zdarzeń do pliku

W celu wyeksportowania zdarzeń do pliku:

1. Uruchom wybór zdarzeń.
2. Zaznacz pole obok żądanego zdarzenia.
3. Kliknij przycisk **Eksportuj do pliku**.

Wybrane zdarzenie zostanie wyeksportowane do pliku.

Przeglądanie historii obiektu ze zdarzenia

Ze zdarzenia utworzenia lub modyfikacji obiektu, które obsługuje zarządzanie rewizją, możesz przełączyć się na historię rewizji obiektu.

W celu przejrzenia historii obiektu ze zdarzenia:

1. Uruchom wybór zdarzeń.

2. Zaznacz pole obok żądanego zdarzenia.

3. Kliknij przycisk **Historia rewizji**.

   Historia rewizji obiektu zostanie otwarta.

Usuwanie zdarzeń

W celu usunięcia jednego lub kilku zdarzeń:

1. Uruchom wybór zdarzeń.

2. Zaznacz pola obok żądanych zdarzeń.

3. Kliknij przycisk **Usuń**.

   Wybrane zdarzenia zostaną usunięte i nie można ich przywrócić.

Usuwanie wyborów zdarzeń

Możesz usuwać tylko wybory zdarzeń zdefiniowane przez użytkownika. Predefiniowanych wyborów zdarzeń nie można usunąć.

W celu usunięcia jednego lub kilku wyborów zdarzeń:

1. W menu głównym przejdź do **Monitorowanie i raportowanie → Wybory zdarzeń**.

2. Zaznacz pola obok wyborów zdarzeń, które chcesz usunąć.

3. Kliknij **Usuń**.

4. W otwartym oknie potwierdzenia kliknij **OK**.

   Wybór zdarzenia zostanie usunięty.

Ustawianie czasu przechowywania dla zdarzenia

Kaspersky Security Center umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego. Konieczne może być przechowywanie niektórych zdarzeń przez dłuższy lub krótszy okres niż określony przez domyślne wartości. Możesz zmienić domyślne ustawienia czasu przechowywania zdarzenia.

Jeśli nie masz zamiaru przechowywać niektórych zdarzeń w bazie danych Serwera administracyjnego, możesz wyłączyć odpowiednie ustawienie w zasadzie Serwera administracyjnego oraz w zasadzie aplikacji Kaspersky lub we właściwościach Serwera administracyjnego (tylko dla zdarzeń Serwera administracyjnego). Zmniejszy to liczbę typów zdarzeń w bazie danych.

Im dłuższy okres przechowywania zdarzenia, tym szybciej baza danych osiągnie maksymalną pojemność. Jednakże dłuższy okres przechowywania zdarzenia umożliwia monitorowanie i raportowanie zadań dla dłuższego przedziału czasu.

W celu skonfigurowania czasu przechowywania zdarzenia w bazie danych Serwera administracyjnego:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Wykonaj jedną z poniższych czynności:
   - Aby skonfigurować okres przechowywania zdarzeń Agenta sieciowego lub zarządzanej aplikacji firmy Kaspersky, kliknij nazwę odpowiedniej zasady.

     Zostanie otwarte okno właściwości zasady.
   - Aby skonfigurować zdarzenia Serwera administracyjnego, w menu głównym kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

     Jeśli masz zasadę dla Serwera administracyjnego, zamiast tego możesz kliknąć nazwę tej zasady.

     Zostanie otwarta strona właściwości Serwera administracyjnego (lub strona właściwości zasady Serwera administracyjnego).
3. Wybierz zakładkę **Konfiguracja zdarzenia**.

   Zostanie wyświetlona lista typów zdarzeń dotyczących sekcji **Krytyczny**.
4. Wybierz sekcję **Błąd funkcjonalny**, **Ostrzeżenie** lub **Informacja**.
5. Na liście typów zdarzeń w prawej części okna kliknij odnośnik dla zdarzenia, którego okres przechowywania chcesz zmienić.

   W sekcji **Rejestracja zdarzenia** otwartego okna włączona jest opcja **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**.
6. W polu edycji znajdującym się pod tym przyciskiem przełącznika wprowadź liczbę dni, przez jaką zdarzenie ma być przechowywane.
7. Jeśli nie chcesz przechowywać zdarzenia w bazie danych Serwera administracyjnego, wyłącz opcję **Przechowuj w bazie danych Serwera administracyjnego przez (dni)**.

   Jeśli konfigurujesz zdarzenia Serwera administracyjnego w oknie właściwości Serwera administracyjnego i jeśli ustawienia zdarzeń są blokowane w zasadzie Serwera administracyjnego Kaspersky Security Center, nie możesz ponownie zdefiniować wartości okresu przechowywania dla zdarzenia.
8. Kliknij **OK**.

   Okno właściwości zasady zostanie zamknięte.

Od tej chwili, gdy serwer administracyjny odbiera i przechowuje zdarzenia wybranego typu, będą one miały zmieniony okres przechowywania. Serwer administracyjny nie zmienia okresu przechowywania wcześniej odebranych zdarzeń.

Typy zdarzeń

Każdy komponent Kaspersky Security Center posiada swój zestaw typów zdarzeń. Ta sekcja zawiera listy typów zdarzeń, które wystąpiły w trakcie działania Serwera administracyjnego Kaspersky Security Center, Agenta sieciowego, serwera iOS MDM oraz serwera urządzeń mobilnych Exchange. Typy zdarzeń, które występują w aplikacjach Kaspersky, nie zostały wymienione w tej sekcji.

Struktura danych opisu typu zdarzeń

Dla każdego typu zdarzenia dostarczone są następujące elementy: wyświetlana nazwa, identyfikator (ID), kod alfabetyczny, opis oraz domyślny czas przechowywania.

- **Nazwa wyświetlanego typu zdarzenia**. Ten tekst jest wyświetlany w Kaspersky Security Center, gdy konfigurujesz zdarzenia oraz podczas występowania zdarzeń.
- **ID typu zdarzenia**. Ten kod numeryczny jest używany, gdy przetwarzasz zdarzenia przy użyciu narzędzi firm trzecich do analizy zdarzeń.
- **Typ zdarzenia** (kod alfabetyczny). Ten kod jest używany, gdy przeglądasz i przetwarzasz zdarzenia, korzystając z widoków publicznych, dostępnych w bazie danych Kaspersky Security Center, a także podczas eksportowania zdarzeń do systemu SIEM.
- **Opis**. Ten tekst zawiera sytuacje, gdy zdarzenie wystąpi i co należy zrobić w takiej sytuacji.
- **Domyślny czas przechowywania**. To jest liczba dni, przez jaką zdarzenie jest przechowywane w bazie danych Serwera administracyjnego i jest wyświetlane na liście zdarzeń na Serwerze administracyjnym. Po upłynięciu tego czasu, zdarzenie jest usuwane. Jeśli wartość czasu przechowywania zdarzenia to 0, takie zdarzenia są wykrywane, ale nie są wyświetlane na liście zdarzeń na Serwerze administracyjnym. Jeśli skonfigurowałeś zapisywanie takich zdarzeń w dzienniku zdarzeń systemu operacyjnego, znajdziesz je tam.

  Możesz zmienić czas przechowywania zdarzeń:

  - Konsola administracyjna: Ustawianie czasu przechowywania dla zdarzenia
  - Kaspersky Security Center Web Console: Ustawianie czasu przechowywania dla zdarzenia

Inne dane mogą zawierać następujące pola:

- **event_id**: unikatowa liczba zdarzeń w bazie danych, wygenerowana i przypisana automatycznie; nie mylić z **ID typu zdarzenia**.
- **task_id**: identyfikator zadania, które spowodowało wystąpienie zdarzenia (jeśli są jakiekolwiek)
- **severity**: jeden z następujących priorytetów (w kolejności rosnącej):

  0) Niepoprawny priorytet

  1) Informacja

  2) Ostrzeżenie

  3) Błąd

  4) Krytyczny

Zdarzenia Serwera administracyjnego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Serwera administracyjnego.

Zdarzenia krytyczne Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Serwera administracyjnego Kaspersky Security Center, które posiadają priorytet **Krytyczny**.

Zdarzenia krytyczne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domy przech
Limit licencji został przekroczony	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Raz dziennie Kaspersky Security Center sprawdza, czy ograniczenia licencyjne nie są przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją przekracza 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod	180 dn

			aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center określa reguły generowania zdarzeń, gdy ograniczenia licencjonowania zostaną przekroczone.	
Epidemia wirusa	26 (dla Ochrony plików)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dn
Epidemia wirusa	27 (dla Ochrony poczty)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach	180 dn

			Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	
Epidemia wirusa	28 (dla Zapory sieciowej)	GNRL_EV_VIRUS_OUTBREAK	Zdarzenia tego typu występują, gdy liczba szkodliwych obiektów, wykrytych na kilku zarządzanych urządzeniach przekracza wartość progową w krótkim przedziale czasu. Możesz zareagować na zdarzenie w następujące sposoby: • Skonfiguruj wartość progową we właściwościach Serwera administracyjnego. • Utwórz rygorystyczną zasadę, która zostanie aktywowana, lub utwórz zadanie, które zostanie uruchomione przy wystąpieniu tego zdarzenia.	180 dn
Zarządzanie urządzeniem nie jest możliwe	4111	KLSRV_HOST_OUT_CONTROL	Zdarzenia tego typu występują, jeśli zarządzane urządzenie jest widoczne w sieci, ale nie ma podłączonego Serwera administracyjnego przez pewien czas.	180 dn

			Dowiedz się, co uniemożliwia poprawne działanie Agenta sieciowego na urządzeniu. Możliwe przyczyny obejmują problemy z siecią i usuwanie Agenta sieciowego z urządzenia.	
Stan urządzenia: Krytyczny	4113	KLSRV_HOST_STATUS_CRITICAL	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Krytyczny*. Możesz skonfigurować warunki, zgodnie z którymi stan urządzenia zostanie zmieniony na *Krytyczny*.	180 dn
Plik klucza został dodany do listy zablokowanych	4124	KLSRV_LICENSE_BLACKLISTED	Zdarzenia tego typu występują, gdy firma Kaspersky dodała kod aktywacyjny lub plik klucza, którego używasz, do listy blokowanych. Aby uzyskać więcej informacji, skontaktuj się z działem pomocy technicznej.	180 dn
Tryb ograniczonej funkcjonalności	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Zdarzenia tego typu występują, gdy Kaspersky Security Center zaczyna działać z podstawową funkcjonalnością, bez funkcji Zarządzanie lukami i poprawkami oraz bez funkcji Zarządzanie urządzeniami mobilnymi. Poniższe elementy są przyczynami i odpowiednimi odpowiedziami na zdarzenie: • Licencja utraciła ważność. Zapewnij licencję do korzystania z trybu pełnej funkcjonalności Kaspersky Security	180 dn

			Center (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). • Serwer administracyjny zarządza większą liczbą urządzeń niż określona przez ograniczenie licencji. Przenieś urządzenia z grup administracyjnych Serwera administracyjnego do tych należących do innego Serwera administracyjnego (jeśli ograniczenie licencji innego Serwera administracyjnego zezwala na to).	
Licencja wkrótce utraci ważność	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Tego typu zdarzenia mają miejsce, gdy zbliża się data wygaśnięcia licencji komercyjnej. Raz dziennie Kaspersky Security Center sprawdza, czy nie zbliża się data wygaśnięcia licencji. Wydarzenia tego typu publikowane są 30 dni, 15 dni, 5 dni i 1 dzień przed datą wygaśnięcia licencji. Nie możesz zmienić liczby dni. Jeśli Serwer administracyjny zostanie wyłączony określonego dnia przed datą wygaśnięcia licencji, zdarzenie nie zostanie opublikowane, aż do następnego dnia. Po wygaśnięciu licencji komercyjnej Kaspersky Security Center zapewnia tylko podstawową funkcjonalność.	180 dn

			Możesz zareagować na zdarzenie w następujące sposoby: • Upewnij się, że zapasowy klucz licencyjny został dodany do Serwera administracyjnego. • Jeśli korzystasz z subskrypcji, pamiętaj o jej odnowieniu. Nieograniczona subskrypcja jest odnawiana automatycznie, jeśli została opłacona w odpowiednim terminie.	
Certyfikat wygasł	4132	KLSRV_CERTIFICATE_EXPIRED	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla Zarządzania urządzeniami mobilnymi utraci ważność. Należy zaktualizować certyfikat, który utracił ważność. Możesz skonfigurować automatyczne aktualizacje certyfikatów, zaznaczając pole **Odnów certyfikat automatycznie, jeśli jest to możliwe** w ustawieniach wydawania certyfikatów.	180 dn
Aktualizacje dla modułów oprogramowania Kaspersky zostały wycofane	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Zdarzenia tego typu występują, jeśli aktualizacje typu seamless zostały wycofane (dla tych aktualizacji wyświetlany jest stan *Wycofano*) przez specjalistów z pomocy technicznej Kaspersky; na przykład, muszą	180 dn

			zostać zaktualizowane do nowszej wersji. Zdarzenie dotyczy poprawek Kaspersky Security Center i nie dotyczy modułów zarządzanych aplikacji firmy Kaspersky. Zdarzenie zawiera przyczynę niezainstalowania aktualizacji typu seamless.	

Zdarzenia błędu funkcyjnego Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Błąd funkcjonalny**.

Zdarzenia błędu funkcyjnego Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyś przecho
Błąd w czasie wykonywania	4125	KLSRV_RUNTIME_ERROR	Zdarzenia tego typu występują w wyniku nieznanych problemów. Najczęściej są to problemy z systemem DBMS, problemy z siecią oraz inne problemy z oprogramowaniem i sprzętem. Szczegóły zdarzenia można znaleźć w opisie zdarzenia.	180 dni
Przekroczono limit instalacji dla jednej z grup licencjonowanych aplikacji	4126	KLSRV_INVLICPROD_EXCEDED	Serwer administracyjny generuje zdarzenia tego typu okresowo (co godzinę). Zdarzenia tego typu występują, jeśli w Kaspersky Security Center zarządzasz kluczami licencyjnymi aplikacji innych firm i jeśli liczba instalacji przekroczyła ograniczenie ustawione przez klucz licencyjny aplikacji innej firmy.	180 dni

			Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń aplikację innej firmy z urządzeń, na których aplikacja nie jest używana. • Użyj licencji innej firmy dla większej liczby urządzeń. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji. Grupa licencjonowanych aplikacji zawiera aplikacje firm trzecich spełniające kryteria ustalone przez Ciebie.	
Przeszukanie segmentu chmury nie powiodło się	4143	KLSRV_KLCLOUD_SCAN_ERROR	Zdarzenia tego typu mają miejsce, gdy serwer administracyjny nie może przeszukać segmentu sieci w środowisku chmury. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio.	Nie jest przecho
Kopiowanie aktualizacji do określonego folderu nie powiodło się	4123	KLSRV_UPD_REPL_FAIL	Zdarzenia tego typu występują, gdy aktualizacje oprogramowania są kopiowane do dodatkowych folderów współdzielonych. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy konto użytkownika, który ma uzyskać dostęp do folderu(ów)	180 dni

			posiada prawo do zapisu. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu(ów) uległy zmianie. • Sprawdź połączenie z internetem, gdyż to może być przyczyną zdarzenia. Aby zaktualizować bazy danych i moduły oprogramowania, postępuj zgodnie z instrukcjami.	
Brak wolnego miejsca na dysku	4107	KLSRV_DISK_FULL	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	180 dni
Folder współdzielony nie jest dostępny	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Zdarzenia tego typu występują, jeśli folder współdzielony Serwera administracyjnego jest niedostępny. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy Serwer administracyjny (na którym znajduje się folder współdzielony) jest włączony i dostępny. • Sprawdź, czy nazwa użytkownika i/lub hasło do folderu uległy zmianie.	180 dni

			• Sprawdź połączenie sieciowe.	
Baza danych Serwera administracyjnego jest niedostępna	4109	KLSRV_DATABASE_UNAVAILABLE	Zdarzenia tego typu występują, jeśli baza danych Serwera administracyjnego stała się niedostępna. Możesz zareagować na zdarzenie w następujące sposoby: • Sprawdź, czy zdalny serwer, na którym jest zainstalowany serwer SQL, jest dostępny. • Przejrzyj raporty systemu DBMS, aby odkryć przyczynę braku dostępności bazy danych Serwera administracyjnego. Na przykład, ze względu na profilaktyczną obsługę, zdalny serwer z zainstalowanym serwerem SQL może być niedostępny.	180 dni
Brak wolnego miejsca w bazie danych Serwera administracyjnego	4110	KLSRV_DATABASE_FULL	Zdarzenia tego typu występują, gdy nie ma wolnego miejsca w bazie danych Serwera administracyjnego. Serwer administracyjny nie działa, gdy jego baza danych osiągnęła swoją pojemność i gdy dalsze zapisywanie w bazie danych nie jest możliwe.	180 dni

			Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie: • Korzystasz z SQL Server Express Edition DBMS: W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego przekroczyła ograniczenie rozmiaru bazy danych. Ograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. W bazie danych Serwera administracyjnego istnieje zbyt dużo zdarzeń wysłanych przez komponent Kontrola aplikacji. Możesz zmienić ustawienia zasady Kaspersky Endpoint Security for Windows dotyczące przechowywania zdarzeń Kontroli aplikacji w bazie danych Serwera administracyjnego. • Używasz systemu DBMS innego niż SQL Server Express Edition:

			Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Zmniejszanie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	

Zdarzenia ostrzegające Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Ostrzeżenie**.

Zdarzenia ostrzegające Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Do prze
Limit licencji został przekroczony	4098	KLSRV_EV_LICENSE_CHECK_100_110	Raz dziennie Kaspersky Security Center sprawdza, czy ograniczenia licencyjne nie są przekroczone. Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją stanowi od 100% do 110% całkowitej liczby jednostek objętych licencją.	90 d

			Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center określa reguły generowania zdarzeń, gdy ograniczenia licencjonowania zostaną przekroczone.	
Urządzenie było nieaktywne w sieci od dłuższego czasu	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan Ostrzeżenie. Najczęściej dzieje się tak, gdy zarządzane urządzenie zostaje wycofane z eksploatacji. Możesz zareagować na zdarzenie w następujące sposoby: • W celu usunięcia urządzenia z listy zarządzanych urządzeń: • Określ przedział czasu, po którym tworzone jest zdarzenie **Urządzenie było nieaktywne w sieci od dłuższego czasu**, przy użyciu Konsoli administracyjnej	90 d

			lub przy użyciu Kaspersky Security Center Web Console. • Określ przedział czasu, po którym urządzenie zostanie automatycznie usunięte z grupy, przy użyciu Konsoli administracyjnej lub Kaspersky Security Center Web Console.	
Konflikt nazw urządzeń	4102	KLSRV_EVENT_HOSTS_CONFLICT	Zdarzenia tego typu występują, gdy Serwer administracyjny traktuje dwa lub więcej zarządzanych urządzeń jako jedno urządzenie. Ma to miejsce najczęściej wtedy, gdy sklonowany dysk twardy został użyty do wdrożenia oprogramowania na zarządzanych urządzeniach i bez przełączania Agenta sieciowego do trybu klonowania dedykowanego dysku na odpowiednim urządzeniu. Aby uniknąć tego problemu, przełącz Agenta sieciowego do trybu klonowania dysku na odpowiednim urządzeniu przed sklonowaniem dysku twardego tego urządzenia.	90 c
Stan urządzenia: Ostrzeżenie	4114	KLSRV_HOST_STATUS_WARNING	Zdarzenia tego typu występują, gdy do zarządzanego urządzenia zostanie przypisany stan *Ostrzeżenie*. Możesz skonfigurować warunki, zgodnie z którymi stan urządzenia zostanie	90 c

			zmieniony na *Ostrzeżenie*.	
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony	4127	KLSRV_INVLICPROD_FILLED	Zdarzenia tego typu występują, gdy liczba instalacji aplikacji innych firm, zawartych w grupie licencjonowanych aplikacji osiągnie 90% maksymalnej dozwolonej wartości określonej we właściwościach klucza licencyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Jeśli aplikacja innej firmy nie jest używana na niektórych zarządzanych urządzeniach, usuń aplikację z tych urządzeń. • Jeśli spodziewasz się, że w najbliższej przyszłości liczba instalacji dla aplikacji innej firmy przekroczy dozwoloną maksymalną wartość, uwzględnij uzyskanie licencji innej firmy dla większej liczby urządzeń w przyszłości. Możesz zarządzać kluczami licencyjnymi aplikacji firm trzecich, korzystając z funkcjonalności grup licencjonowanych aplikacji.	90 c
Certyfikat został zażądany	4133	KLSRV_CERTIFICATE_REQUESTED	Zdarzenia tego typu występują, gdy certyfikat dla Zarządzania urządzeniami mobilnymi nie zostanie automatycznie wystawiony ponownie.	90 c

			Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Automatyczne ponowne wystawienie zostało zainicjowane dla certyfikatu, dla którego wyłączona jest opcja **Odnów certyfikat automatycznie, jeśli jest to możliwe**. Może to być spowodowane błędem, który wystąpił podczas tworzenia certyfikatu. Konieczne może być ręczne ponowne wystawienie certyfikatu. • Jeśli korzystasz z integracji z infrastrukturą klucza publicznego, przyczyną może być brak atrybutu SAM-Account-Name konta użytego do integracji z PKI oraz do wystawienia certyfikatu. Przejrzyj właściwości konta.	
Certyfikat został usunięty	4134	KLSRV_CERTIFICATE_REMOVED	Zdarzenia tego typu występują, gdy administrator usunie dowolny typ certyfikatu (Ogólny, Poczta, VPN) dla Zarządzania urządzeniami mobilnymi.	90 c

			Po usunięciu certyfikatu urządzenia mobilne, podłączone za pośrednictwem tego certyfikatu, nie nawiążą połączenia z Serwerem administracyjnym. To zdarzenie może być pomocne podczas sprawdzania problemów z działaniem, skojarzonych z zarządzaniem urządzeń mobilnych.	
Certyfikat APNs wygasł	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Zdarzenia tego typu występują, gdy certyfikat APNs utraci ważność. Należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM.	Nie prze
Certyfikat APNs wkrótce utraci ważność	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Zdarzenia tego typu występują, gdy do wygaśnięcia certyfikatu APNs pozostało mniej niż 14 dni. Jeśli certyfikat APNs utraci ważność, należy ręcznie odnowić certyfikat APNs i zainstalować go na serwerze iOS MDM. Zalecane jest wcześniejsze utworzenie terminarza odnawiania certyfikatu APNs.	Nie prze
Błąd podczas przesyłania wiadomości FCM do urządzenia mobilnego	4138	KLSRV_GCM_DEVICE_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Google Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android,	90 c

			a FCM Server nie obsłuży żądań otrzymanych z Serwera administracyjnego. To oznacza, że niektóre zarządzane urządzenia mobilne nie otrzymają powiadomienia push. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z FCM Server i powiązanych błędów można znaleźć w dokumentacji do usługi Google Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie").	
Błąd HTTP podczas wysyłania wiadomości FCM do serwera FCM	4139	KLSRV_GCM_HTTP_ERROR	Zdarzenia tego typu występują, gdy Zarządzanie urządzeniami mobilnymi jest skonfigurowane do użycia Google Firebase Cloud Messaging (FCM) w celu połączenia z zarządzanymi urządzeniami mobilnymi z systemem operacyjnym Android, a FCM Server przywróci żądanie Serwera administracyjnego z kodem HTTP innym niż 200 (OK). Poniżej znajdują się możliwe przyczyny wystąpienia tego zdarzenia oraz odpowiednie reakcje na nie: • Problemy po stronie serwera FCM. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio.	90 c

			Więcej informacji na temat kodów HTTP otrzymanych z FCM Server i powiązanych błędów można znaleźć w dokumentacji do usługi Google Firebase (zajrzyj do rozdziału „Podrzędne kody odpowiedzi na komunikaty o błędzie"). • Problemy po stronie serwera proxy (jeśli korzystasz z serwera proxy). Przeczytaj kod HTTP w szczegółach zdarzenia i zareaguj odpowiednio.	
Błąd podczas przesyłania wiadomości FCM do serwera FCM	4140	KLSRV_GCM_GENERAL_ERROR	Zdarzenia tego typu występują w wyniku niespodziewanych błędów po stronie Serwera administracyjnego podczas pracy z protokołem Google Firebase Cloud Messaging HTTP. Przeczytaj szczegóły w opisie zdarzenia i zareaguj odpowiednio. Jeżeli nie znajdziesz rozwiązania swojego problemu, skontaktuj się z działem pomocy technicznej firmy Kaspersky.	90 d
Pozostała niewielka ilość wolnego miejsca na dysku twardym	4105	KLSRV_NO_SPACE_ON_VOLUMES	Tego typu zdarzenia występują, gdy dysk twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, prawie zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	90 d

Mała ilość wolnego miejsca w bazie danych Serwera administracyjnego	4106	KLSRV_NO_SPACE_IN_DATABASE	Zdarzenia tego typu występują, jeśli miejsce w bazie danych Serwera administracyjnego jest zbyt ograniczone. Jeśli nie rozwiążesz tego problemu, wkrótce baza danych Serwera administracyjnego osiągnie swoją pojemność, a Serwer administracyjny nie będzie działał. Poniżej wymienione są przyczyny tego zdarzenia, w zależności od systemu DBMS, którego używasz, oraz odpowiednie reakcje na to zdarzenie. Korzystasz z SQL Server Express Edition DBMS: • W dokumentacji SQL Server Express sprawdź ograniczenie rozmiaru bazy danych dla wersji, której używasz. Prawdopodobnie Twoja baza danych Serwera administracyjnego zaraz osiągnie ograniczenie rozmiaru bazy danych. • Ograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • W bazie danych Serwera administracyjnego istnieje zbyt dużo zdarzeń wysłanych przez komponent Kontrola aplikacji. Możesz zmienić ustawienia zasady Kaspersky	90 d

			Endpoint Security for Windows dotyczące przechowywania zdarzeń Kontroli aplikacji w bazie danych Serwera administracyjnego. Używasz systemu DBMS innego niż SQL Server Express Edition: • Nieograniczanie liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego. Przeglądanie informacji dotyczących wyboru systemu DBMS.	
Połączenie z podrzędnym Serwerem administracyjnym zostało zerwane	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z podrzędnym Serwerem administracyjnym zostanie przerwane. Przeczytaj dziennik zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany podrzędny Serwer administracyjny i zareaguj odpowiednio.	90 c
Połączenie z głównym Serwerem administracyjnym zostało zerwane	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Zdarzenia tego typu występują, gdy połączenie z głównym Serwerem administracyjnym zostanie przerwane.	90 c

			Przeczytaj dziennik zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany główny Serwer administracyjny i zareaguj odpowiednio.	
Zarejestrowano nowe aktualizacje dla modułów oprogramowania Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Zdarzenia tego typu występują, gdy Serwer administracyjny zarejestruje nowe aktualizacje dla oprogramowania firmy Kaspersky, zainstalowanego na zarządzanych urządzeniach, których instalacja wymaga zatwierdzenia. Zatwierdź lub odrzuć aktualizacje, korzystając z Konsoli administracyjnej lub Kaspersky Security Center Web Console.	90 d
Przekroczono limit wydarzeń w bazie danych. Rozpoczęto usuwanie wydarzeń	4145	KLSRV_EVP_DB_TRUNCATING	Zdarzenia tego typu występują, jeśli usuwanie starszych zdarzeń z bazy danych Serwera administracyjnego rozpoczęło się, gdy pojemność bazy danych Serwera administracyjnego została osiągnięta. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	Nie j prze
Przekroczono	4146	KLSRV_EVP_DB_TRUNCATED	Zdarzenia tego typu	Nie j

limit wydarzeń w bazie danych. Usunięto wydarzenia			występują, jeśli starsze zdarzenia zostały usunięte z bazy danych Serwera administracyjnego po osiągnięciu pojemności bazy danych Serwera administracyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej dozwolonej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	prze

Zdarzenia informacyjne Serwera administracyjnego

Poniższa tabela prezentuje zdarzenia Serwera administracyjnego Kaspersky Security Center, których istotność to **Informacja**.

Zdarzenia informacyjne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Ponad 90% tego klucza licencyjnego jest wykorzystane	4097	KLSRV_EV_LICENSE_CHECK_90	30 dni
Wykryto nowe urządzenie	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 dni
Urządzenie zostało automatycznie dodane do grupy	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 dni
Urządzenie zostało usunięte z grupy: nieaktywność w sieci od dłuższego czasu	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 dni
Limit instalacji w jednej z grup licencjonowanych aplikacji zostanie wkrótce przekroczony (wykorzystywanych jest więcej niż 95%)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 dni
Wykryto pliki do przesłania	4131	KLSRV_APS_FILE_APPEARED	30 dni

do firmy Kaspersky w celu analizy			
ID instancji FCM na tym urządzeniu mobilnym zmieniło się	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 dni
Aktualizacje zostały pomyślnie skopiowane do wskazanego folderu	4122	KLSRV_UPD_REPL_OK	30 dni
Nawiązano połączenie z podrzędnym Serwerem administracyjnym	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 dni
Nawiązano połączenie z głównym Serwerem administracyjnym	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 dni
Bazy danych zostały zaktualizowane	4144	KLSRV_UPD_BASES_UPDATED	30 dni
Audyt: Połączenie z Serwerem administracyjnym zostało nawiązane	4147	KLAUD_EV_SERVERCONNECT	30 dni
Audyt: Obiekt został zmodyfikowany	4148	KLAUD_EV_OBJECTMODIFY	30 dni
Audyt: Stan obiektu zmienił się	4150	KLAUD_EV_TASK_STATE_CHANGED	30 dni
Audyt: Ustawienia grupy zostały zmodyfikowane	4149	KLAUD_EV_ADMGROUP_CHANGED	30 dni
Audyt: Połączenie z Serwerem administracyjnym zostało zakończone	4151	KLAUD_EV_SERVERDISCONNECT	30 dni
Audyt: Właściwości obiektu zostały zmodyfikowane	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 dni
Audyt: uprawnienia użytkownika zostały zmodyfikowane	4153	KLAUD_EV_OBJECTACLMODIFIED	30 dni
Audyt: Klucze szyfrowania zostały zaimportowane lub wyeksportowane z Serwera administracyjnego	5100	KLAUD_EV_DPEKEYSEXPORT	30 dni

Zdarzenia Agenta sieciowego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Agenta sieciowego.

Zdarzenia błędu funkcyjnego Agenta sieciowego

Poniższa tabela wyświetla typy zdarzeń Agenta sieciowego Kaspersky Security Center, których priorytet to **Błąd funkcjonalny**.

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyślny cz przechowywa
Błąd podczas instalacji aktualizacji	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli automatyczne aktualizowanie i instalowanie poprawek dla składników Kaspersky Security Center nie zakończyło się pomyślnie. Zdarzenie nie dotyczy aktualizacji zarządzanych aplikacji firmy Kaspersky. Przeczytaj opis zdarzenia. Przyczyną tego zdarzenia może być problem z systemem Windows na Serwerze administracyjnym. Jeśli w opisie wspomniany jest jakikolwiek problem z konfiguracją systemu Windows, rozwiąż ten problem.	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej nie powiodła się	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli używane są funkcje Zarządzanie lukami i poprawkami i Zarządzanie urządzeniami mobilnymi oraz jeśli aktualizacja oprogramowania innych firm nie zakończyła się pomyślnie.	30 dni

			Sprawdź, czy odnośnik do oprogramowania innej firmy jest ważny. Przeczytaj opis zdarzenia.	
Zainstalowanie aktualizacji Windows Update nie powiodło się	7717	KLNAG_EV_WUA_INSTALL_ERROR	Zdarzenia tego typu występują, jeśli aktualizacje systemu Windows nie zakończyły się pomyślnie. Konfiguruj aktualizacji systemu Windows w profilu Agenta sieciowego. Przeczytaj opis zdarzenia. Poszukaj błędu w Bazie wiedzy Microsoft. Skontaktuj się z pomocą techniczną Microsoft, jeśli sam nie możesz rozwiązać problemu.	30 dni

Zdarzenia ostrzegające Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center, które posiadają priorytet **Ostrzeżenie**.

Zdarzenia ostrzegające Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Proces instalacji aktualizacji modułów oprogramowania zwrócił ostrzeżenie	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została zakończona ostrzeżeniem	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została odroczona	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 dni
Wystąpił incydent	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 dni

dostępności KSN nie powiodło się			

Zdarzenia informacyjne Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center, które posiadają priorytet **Informacja**.

Zdarzenia informacyjne Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Aktualizacja modułów aplikacji została pomyślnie zainstalowana	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Instalacja aktualizacji modułów oprogramowania została uruchomiona	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 dni
Aplikacja została zainstalowana	7703	KLNAG_EV_INV_APP_INSTALLED	30 dni
Aplikacja została odinstalowana	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 dni
Monitorowana aplikacja została zainstalowana	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 dni
Monitorowana aplikacja została odinstalowana	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 dni
Aplikacja innego producenta została zainstalowana	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 dni
Dodano nowe urządzenie	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dni
Urządzenie zostało usunięte	7709	KLNAG_EV_DEVICE_REMOVE	30 dni
Wykryto nowe urządzenie	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dni
Urządzenie zostało zautoryzowane	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dni
Udostępnianie pulpitu Windows: Plik został odczytany	7712	KLUSRLOG_EV_FILE_READ	30 dni
Udostępnianie	7713	KLUSRLOG_EV_FILE_MODIFIED	30 dni

pulpitu Windows: Plik został zmodyfikowany			
Udostępnianie pulpitu Windows: Aplikacja została uruchomiona	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 dni
Udostępnianie pulpitu Windows: Uruchomiono	7715	KLUSRLOG_EV_WDS_BEGIN	30 dni
Udostępnianie pulpitu Windows: Zatrzymano	7716	KLUSRLOG_EV_WDS_END	30 dni
Aktualizacja oprogramowania firmy trzeciej została pomyślnie zainstalowana	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 dni
Instalacja aktualizacji oprogramowania firmy trzeciej została uruchomiona	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 dni
Serwer KSN proxy został uruchomiony. Sprawdzenie dostępności KSN zostało pomyślnie zakończone	7719	KSNPROXY_STARTED_CON_CHK_OK	30 dni
KSN Proxy został zatrzymany	7720	KSNPROXY_STOPPED	30 dni

Zdarzenia serwera iOS MDM

Ta sekcja zawiera informacje o zdarzeniach dotyczących serwera iOS MDM.

Zdarzenia błedu funkcjonalnego serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Błąd funkcjonalny**.

Zdarzenia błedu funkcjonalnego serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Pobranie listy profili nie powiodło się	PROFILELIST_COMMAND_FAILED	30 dni
Instalacja profilu nie powiodła się	INSTALLPROFILE_COMMAND_FAILED	30 dni

Usunięcie profilu nie powiodło się	REMOVEPROFILE_COMMAND_FAILED	30 dni
Pobranie listy profili informacyjnych nie powiodło się	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 dni
Instalacja profilu informacyjnego nie powiodła się	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu informacyjnego nie powiodło się	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 dni
Usunięcie profilu informacyjnego nie powiodło się	CERTIFICATELIST_COMMAND_FAILED	30 dni
Pobranie listy zainstalowanych aplikacji nie powiodło się	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 dni
Pobranie ogólnych informacji o urządzeniu mobilnym nie powiodło się	DEVICEINFORMATION_COMMAND_FAILED	30 dni
Pobranie informacji o zabezpieczeniach nie powiodło się	SECURITYINFO_COMMAND_FAILED	30 dni
Zablokowanie urządzenia mobilnego nie powiodło się	DEVICELOCK_COMMAND_FAILED	30 dni
Zresetowanie hasła nie powiodło się	CLEARPASSCODE_COMMAND_FAILED	30 dni
Usunięcie danych z urządzenia mobilnego nie powiodło się	ERASEDEVICE_COMMAND_FAILED	30 dni
Instalacja aplikacji nie powiodła się	INSTALLAPPLICATION_COMMAND_FAILED	30 dni
Ustawienie kodu wykupu dla aplikacji nie powiodło się	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 dni
Pobranie listy zarządzanych aplikacji nie powiodło się	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 dni
Usunięcie zarządzanej aplikacji nie powiodło się	REMOVEAPPLICATION_COMMAND_FAILED	30 dni
Ustawienia roamingu zostały odrzucone	SETROAMINGSETTINGS_COMMAND_FAILED	30 dni
Wystąpił błąd działania aplikacji	PRODUCT_FAILURE	30 dni
Wynik polecenia zawiera niepoprawne dane	MALFORMED_COMMAND	30 dni
Przesłanie powiadomienia push nie powiodło się	SEND_PUSH_NOTIFICATION_FAILED	30 dni
Wysłanie polecenia nie	SEND_COMMAND_FAILED	30 dni

powiodło się		
Nie odnaleziono urządzenia	DEVICE_NOT_FOUND	30 dni

Zdarzenia ostrzegające serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Ostrzeżenie**.

Zdarzenia ostrzegające serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Wykryto próbę podłączenia zablokowanego urządzenia mobilnego	INACTICE_DEVICE_TRY_CONNECTED	30 dni
Profil został usunięty	MDM_PROFILE_WAS_REMOVED	30 dni
Wykryto próbę ponownego użycia certyfikatu klienta	CLIENT_CERT_ALREADY_IN_USE	30 dni
Wykryto nieaktywne urządzenie	FOUND_INACTIVE_DEVICE	30 dni
Wymagany jest kod wykupu	NEED_REDEMPTION_CODE	30 dni
Profil zawarty w zasadach został usunięty z urządzenia	UMDM_PROFILE_WAS_REMOVED	30 dni

Zdarzenia informacyjne serwera iOS MDM

Poniższa tabela wyświetla zdarzenia serwera iOS MDM Kaspersky Security Center, które posiadają priorytet **Informacja**.

Zdarzenia informacyjne serwera iOS MDM

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Podłączono nowe urządzenie mobilne	NEW_DEVICE_CONNECTED	30 dni
Lista profili została pomyślnie pobrana	PROFILELIST_COMMAND_SUCCESSFULL	30 dni
Profil został pomyślnie zainstalowany	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 dni
Profil został pomyślnie usunięty	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 dni
Lista profili informacyjnych została pomyślnie pobrana	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 dni
Profil informacyjny został pomyślnie zainstalowany	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dni
Profil informacyjny został pomyślnie usunięty	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dni

Lista certyfikatów cyfrowych została pomyślnie pobrana	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 dni
Lista zainstalowanych aplikacji została pomyślnie zażądana	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dni
Ogólne informacje o urządzeniu mobilnym zostały pomyślnie pobrane	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 dni
Informacje o zabezpieczeniach zostały pomyślnie pobrane	SECURITYINFO_COMMAND_SUCCESSFULL	30 dni
Urządzenie mobilne zostało pomyślnie zablokowane	DEVICELOCK_COMMAND_SUCCESSFULL	30 dni
Hasło zostało pomyślnie zresetowane	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 dni
Dane zostały pomyślnie usunięte z urządzenia mobilnego	ERASEDEVICE_COMMAND_SUCCESSFULL	30 dni
Aplikacja została pomyślnie zainstalowana	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 dni
Kod wykupu aplikacji został pomyślnie ustawiony dla aplikacji	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 dni
Lista zarządzanych aplikacji została pomyślnie pobrana	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dni
Zarządzana aplikacja została pomyślnie usunięta	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 dni
Ustawienia roamingu zostały pomyślnie zastosowane	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 dni

Zdarzenia serwera urządzeń mobilnych Exchange

Ta sekcja zawiera informacje o zdarzeniach dotyczących serwera urządzeń mobilnych Exchange.

Zdarzenia błędu funkcjonalnego serwera urządzeń mobilnych Exchange

Poniższa tabela wyświetla zdarzenia serwera urządzeń mobilnych Exchange Kaspersky Security Center, które posiadają priorytet **Błąd funkcjonalny**.

Zdarzenia błędu funkcjonalnego serwera urządzeń mobilnych Exchange

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Usunięcie danych z urządzenia mobilnego nie powiodło się	WIPE_FAILED	30 dni
Nie można usunąć informacji o połączeniu urządzeń mobilnych ze skrzynkami pocztowymi	DEVICE_REMOVE_FAILED	30 dni
Zastosowanie profilu ActiveSync w skrzynce pocztowej nie powiodło się	POLICY_APPLY_FAILED	30 dni
Błąd działania aplikacji	PRODUCT_FAILURE	30 dni
Modyfikacja stanu funkcjonalności ActiveSync nie powiodła się	CHANGE_ACTIVE_SYNC_STATE_FAILED	30 dni

Zdarzenia informacyjne serwera urządzeń mobilnych Exchange

Poniższa tabela wyświetla zdarzenia serwera urządzeń mobilnych Exchange Kaspersky Security Center, które posiadają priorytet **Informacja**.

Zdarzenia informacyjne serwera urządzeń mobilnych Exchange

Nazwa wyświetlanego typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Podłączono nowe urządzenie mobilne	NEW_DEVICE_CONNECTED	30 dni
Dane zostały pomyślnie usunięte z urządzenia mobilnego	WIPE_SUCCESSFULL	30 dni

Blokowanie często występujących zdarzeń

Ta sekcja zawiera informacje dotyczące zarządzania blokowaniem często występujących zdarzeń oraz usuwania blokowania często występujących zdarzeń.

Informacje o blokowaniu często występujących zdarzeń

Zarządzana aplikacja, na przykład Kaspersky Endpoint Security for Windows, zainstalowana na jednym lub kilku zarządzanych urządzeniach, może wysyłać wiele zdarzeń tego samego typu do Serwera administracyjnego. Otrzymywanie częstych zdarzeń może przeciążyć bazę danych Serwera administracyjnego i nadpisać inne zdarzenia. Serwer administracyjny zaczyna blokować najczęstsze zdarzenia, gdy liczba wszystkich odebranych zdarzeń przekracza określony limit dla bazy danych.

Serwer administracyjny blokuje automatyczne odbieranie często występujących zdarzeń. Nie możesz samodzielnie blokować często występujących zdarzeń ani wybierać, które zdarzenia mają być blokowane.

Jeśli chcesz dowiedzieć się, czy zdarzenie jest zablokowane, możesz sprawdzić listę powiadomień lub możesz sprawdzić, czy to zdarzenie jest obecne w sekcji **Blokowanie często występujących zdarzeń** właściwości Serwera administracyjnego. Jeśli zdarzenie jest zablokowane, możesz wykonać następujące czynności:

- Jeśli chcesz zapobiec nadpisywaniu bazy danych, możesz kontynuować blokowanie odbieranie tego typu zdarzeń.
- Jeśli chcesz, na przykład, znaleźć przyczynę wysyłania często występujących zdarzeń na Serwer administracyjny, możesz odblokować często występujące zdarzenia i mimo wszystko nadal otrzymywać tego typu zdarzenia.
- Jeśli chcesz nadal otrzymywać często występujące zdarzenia, dopóki nie zostaną ponownie zablokowane, możesz usunąć z blokowania często występujące zdarzenia.

Zarządzanie blokowaniem często występujących zdarzeń

Serwer administracyjny blokuje automatyczne odbieranie często występujących zdarzeń, ale możesz odblokować tę opcję i nadal odbierać często występujące zdarzenia. Możesz także zablokować odbieranie często występujących zdarzeń, które wcześniej odblokowałeś.

W celu zarządzania blokowaniem często występujących zdarzeń:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Blokowanie często występujących zdarzeń**

3. W sekcji **Blokowanie często występujących zdarzeń**:

   - Jeśli chcesz odblokować odbieranie często występujących zdarzeń:

     a. Wybierz często występujące zdarzenia, które chcesz odblokować, a następnie kliknij przycisk **Wyklucz**.

     b. Kliknij przycisk **Zapisz**.

   - Jeśli chcesz zablokować często występujące zdarzenia:

     a. Wybierz często występujące zdarzenia, które chcesz zablokować, a następnie kliknij przycisk **Zablokuj**.

     b. Kliknij przycisk **Zapisz**.

Serwer administracyjny odbiera odblokowane często występujące zdarzenia i nie odbiera zablokowanych często występujących zdarzeń.

Usuwanie blokowania często występujących zdarzeń

Możesz usunąć blokowanie często występujących zdarzeń i rozpocząć ich odbieranie, dopóki Serwer administracyjny nie zablokuje ponownie tych często występujących zdarzeń.

W celu usunięcia blokowania często występujących zdarzeń:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Blokowanie często występujących zdarzeń**

3. W sekcji **Blokowanie często występujących zdarzeń** wybierz typy często występujących zdarzeń, dla których chcesz usunąć blokowanie.

4. Kliknij przycisk **Usuń z blokowania**.

Często występujące zdarzenie zostanie usunięte z listy często występujących zdarzeń. Serwer administracyjny będzie odbierał zdarzenia tego typu.

Odbieranie zdarzeń z Kaspersky Security for Microsoft Exchange Servers

Informacje o zdarzeniach podczas działania zarządzanych aplikacji, takich jak Kaspersky Endpoint Security for Windows, są przesyłane z zarządzanych urządzeń i rejestrowane w bazie danych Serwera administracyjnego. Domyślnie zdarzenia z Kaspersky Security for Microsoft Exchange Servers nie są rejestrowane w bazie danych Serwera administracyjnego. Jeśli Kaspersky Security for Microsoft Exchange Servers jest zainstalowany na zarządzanych urządzeniach w Twojej organizacji i chcesz otrzymywać zdarzenia z tej aplikacji, włącz rejestrację zdarzeń dla tej aplikacji za pomocą narzędzia klscflag.

W celu włączenia rejestracji zdarzeń dla Kaspersky Security for Microsoft Exchange Servers:

1. Na urządzeniu Serwera administracyjnego uruchom wiersz poleceń systemu Windows na koncie z uprawnieniami administratora.

2. Zmień bieżący katalog na folder instalacyjny Kaspersky Security Center (zwykle C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Uruchom jedno z następujących poleceń:

   - Instalowanie Serwera administracyjnego na klastrze trybu failover Microsoft

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Dla Serwera administracyjnego zainstalowanego na węźle klastra pracy awaryjnej Kaspersky:

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Dla Serwera administracyjnego, który nie działa na klastrze:

     ```
     klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
     -v 0
     ```

   Rejestracja zdarzeń dla Kaspersky Security for Microsoft Exchange Servers jest włączona.

W przypadku Kaspersky Security for Microsoft Exchange Servers nie można ustawić okresu przechowywania zdarzeń ani wybrać, które zdarzenia mają zostać zapisane w repozytorium Serwera administracyjnego. Możesz ustawić maksymalną liczbę zdarzeń, które można zapisać w repozytorium. To ustawienie jest stosowane do zdarzeń otrzymanych ze wszystkich aplikacji firmy Kaspersky.

Powiadomienia i stany urządzeń

Ta sekcja zawiera informacje o tym, jak przeglądać powiadomienia, konfigurować dostarczanie powiadomień, używać stanów urządzeń i włączać zmianę stanów urządzeń.

Korzystanie z powiadomień

Powiadomienia informują o zdarzeniach oraz pomagają w przyspieszeniu odpowiedzi na te zdarzenia poprzez wykonanie zalecanych działań lub działań, które uznajesz za odpowiednie.

W zależności od wybranej metody powiadamiania, dostępne są następujące typy powiadomień:

- Powiadomienia na ekranie
- Powiadomienia przez SMS
- Powiadomienia przez e-mail
- Powiadomienia przez uruchomienie pliku wykonywalnego lub skryptu

Powiadomienia na ekranie

Powiadomienia ekranowe informują o zdarzenia pogrupowanych według priorytetów (*Krytyczne*, *Ostrzeżenie* i *Komunikaty informacyjne*).

Powiadomienie ekranowe może przyjąć jeden z dwóch stanów:

- *Przejrzane*. Oznacza to, że wykonałeś zalecane działanie dla powiadomienia lub ręcznie przypisałeś ten stan do powiadomienia.
- *Nieprzejrzane*. Oznacza to, że nie wykonałeś zalecanego działania dla powiadomienia lub nie przypisałeś tego stanu do powiadomienia ręcznie.

Domyślnie, lista powiadomień zawiera powiadomienia ze stanem *Nieprzejrzane*.

Możesz monitorować sieć organizacji, przeglądając powiadomienia ekranowe i odpowiadając na nie w czasie rzeczywistym.

Powiadomienia przez e-mail, przez SMS i przez plik wykonywalny lub skrypt

Kaspersky Security Center oferuje możliwość monitorowania sieci organizacji, wysyłając powiadomienia o zdarzeniu, które uważasz za ważne. Dla każdego zdarzenia możesz skonfigurować powiadomienia przez e-mail, przez SMS lub przez uruchomienie pliku wykonywalnego lub skryptu.

Po otrzymaniu powiadomień przez e-mail lub przez SMS, możesz zdecydować, jaka będzie odpowiedź na zdarzenie. Ta odpowiedź powinna być najbardziej odpowiednia dla sieci Twojej organizacji. Uruchamiając plik wykonywalny lub skrypt, wcześniej definiujesz odpowiedź na zdarzenie. Możesz także rozważyć uruchomienie pliku wykonywalnego lub skryptu jako głównej odpowiedzi na zdarzenie. Po uruchomieniu pliku wykonywalnego, możesz podjąć inne kroki w celu odpowiedzi na zdarzenie.

Przeglądanie powiadomień na ekranie

Powiadomienia na ekranie można wyświetlać na trzy sposoby:

- W sekcji **Monitorowanie i raportowanie → Powiadomienia**. W tym miejscu możesz przejrzeć powiadomienia dotyczące predefiniowanych kategorii.
- W oddzielnym oknie, które może zostać otwarte niezależnie od sekcji, której używasz w danym momencie. W tym przypadku możesz oznaczyć powiadomienia jako przejrzane.
- W widżecie **Powiadomienia według wybranego priorytetu**, w sekcji **Monitorowanie i raportowanie → Pulpit nawigacyjny**. W widżecie możesz przeglądać tylko powiadomienia o zdarzeniach na poziomach istotności *Krytyczny* i *Ostrzeżenie*.

Możesz wykonywać akcje, na przykład, odpowiadać na zdarzenie.

W celu przejrzenia powiadomień z predefiniowanych kategorii:

1. W menu głównym przejdź do **Monitorowanie i raportowanie → Powiadomienia**.

   Kategoria **Wszystkie powiadomienia** została wybrana w lewej części okna, a w prawej części okna są wyświetlane wszystkie powiadomienia.

2. W lewej części okna wybierz jedną z kategorii:

   - **Wdrażanie**
   - **Urządzenia**
   - **Ochrona**
   - **Aktualizacje** (ta kategoria zawiera powiadomienia dotyczące aplikacji Kaspersky, dostępnych do pobrania, i powiadomienia na temat pobranych aktualizacji antywirusowych baz danych)
   - **Ochrona przed exploitami**
   - **Serwer administracyjny** (ta kategoria obejmuje zdarzenia dotyczące tylko Serwera administracyjnego)
   - **Przydatne odnośniki** (ta kategoria obejmuje odnośniki do zasobów Kaspersky, na przykład pomocy technicznej Kaspersky, forum Kaspersky, strony odnowienia licencji lub Encyklopedii IT Kaspersky)
   - **Aktualności od Kaspersky** (ta kategoria obejmuje informacje o publikacji aplikacji firmy Kaspersky)

   Zostanie wyświetlona lista powiadomień wybranej kategorii. Lista zawiera następujące elementy:

- Ikona związana z tematem powiadomienia: wdrożenie (), ochrona (), aktualizacje (), zarządzanie urządzeniami (), Ochrona przed exploitami (), Serwer administracyjny ().
- Poziom istotności powiadomienia. Wyświetlane są powiadomienia następujących poziomów istotności: **Powiadomienia krytyczne** (), **Powiadomienia ostrzegawcze** (), **Powiadomienia informacyjne**. Powiadomienia na liście są pogrupowane według poziomów istotności.
- **Powiadomienie**. Ta kategoria zawiera opis powiadomienia.
- **Akcja**. Ta kategoria zawiera odnośnik do akcji, której wykonanie zalecamy. Na przykład, klikając ten odnośnik, możesz przejść do repozytorium i zainstalować aplikacje zabezpieczające na urządzeniach lub przejrzeć listę urządzeń lub listę zdarzeń. Po wykonaniu zalecanego działania dla powiadomienia, do tego powiadomienia przypisano stan *Przejrzane*.
- **Zarejestrowany stan**. Ta kategoria zawiera liczbę dni lub godzin, które minęły od momentu, gdy powiadomienie zostało zarejestrowane na Serwerze administracyjnym.

W celu przejrzenia powiadomień ekranowych w oddzielnym oknie według poziomu istotności:

1. W prawym górnym rogu Kaspersky Security Center Web Console kliknij ikonę flagi ().

   Jeśli ikona flagi posiada czerwoną kropkę, oznacza to, że istnieją powiadomienia, które nie zostały przejrzane.

   Zostanie otwarte okno wyświetlające powiadomienia. Domyślnie wybrana jest zakładka **Wszystkie powiadomienia**, a powiadomienia są pogrupowane według poziomów istotności: *Krytyczne*, *Ostrzeżenie* i *Informacja*.

2. Wybierz zakładkę **System**.

   Zostanie wyświetlona lista z powiadomieniami posiadającymi poziom istotności powiadomienia *Krytyczne* () i *Ostrzeżenie* (). Lista powiadomień obejmuje następujące obiekty:

   - Znacznik koloru. Powiadomienia krytyczne są oznaczone na czerwono. Powiadomienia ostrzegające są oznaczone na żółto.
   - Ikona wskazująca temat powiadomienia: wdrożenie (), ochrona (), aktualizacje (), zarządzanie urządzeniami (), Ochrona przed exploitami (), Serwer administracyjny ().
   - Opis powiadomienia.
   - Ikona flagi. Ikona flagi jest szara, jeśli do powiadomień jest przypisany stan *Nieprzejrzane*. Jeśli wybierzesz szarą ikonę flagi i przypiszesz stan *Przejrzane* do powiadomienia, ikona zmieni kolor na biały.
   - Odnośnik do zalecanej akcji. Jeśli po kliknięciu odnośnika wykonasz zalecaną akcję, do powiadomienia zostanie przypisany stan *Przejrzane*.
   - Liczba dni, jaka minęła od daty zarejestrowania powiadomienia na Serwerze administracyjnym.

3. Wybierz zakładkę **Więcej**.

   Zostanie wyświetlona lista powiadomień posiadających poziom istotności *Informacja*.

   Organizacja listy jest taka sama, jak listy na zakładce **System** (zapoznaj się z powyższym opisem). Jedyna różnica to brak znacznika koloru.

Możesz filtrować powiadomienia według dat, gdy zostały zarejestrowane na Serwerze administracyjnym. Użyj pola **Pokaż filtr**, aby zarządzać filtrem.

W celu wyświetlenia powiadomień ekranowych na widżecie:

1. W sekcji **Pulpit nawigacyjny** wybierz **Dodaj lub przywróć widżet sieciowy**.

2. W otwartym oknie kliknij kategorię **Inne**, wybierz widżet **Powiadomienia według wybranego priorytetu** i kliknij Dodaj.

   Teraz widżet pojawi się na zakładce **Pulpit nawigacyjny**. Domyślnie, powiadomienia z poziomem istotności *Krytyczne* są wyświetlane na widżecie.

   Możesz kliknąć przycisk **Ustawienia** na widżecie i zmienić ustawienia widżetu, aby przejrzeć powiadomienia z poziomem istotności *Ostrzeżenie*. Lub możesz dodać inny widżet: **Powiadomienia według wybranego poziomu istotności** z priorytetem *Ostrzeżenie*.

   Lista powiadomień na widżecie jest ograniczona według rozmiaru i zawiera dwa powiadomienia. Te dwa powiadomienia odnoszą się do najnowszych zdarzeń.

Lista powiadomień na widżecie obejmuje następujące obiekty:

- Ikona związana z tematem powiadomienia: wdrożenie (), ochrona (), aktualizacje (), zarządzanie urządzeniami (), Ochrona przed exploitami (), Serwer administracyjny ().
- Opis powiadomienia z odnośnikiem do zalecanej akcji. Jeśli po kliknięciu odnośnika wykonasz zalecaną akcję, do powiadomienia zostanie przypisany stan *Przejrzane*.
- Liczbę dni lub liczbę godzin, które minęły od daty zarejestrowania powiadomienia na Serwerze administracyjnym.
- Odnośnik do innych powiadomień. Po kliknięciu tego odnośnika, zostajesz przeniesiony do widoku powiadomień w sekcji **Powiadomienia** sekcji **Monitorowanie i raportowanie**.

Informacje o stanach urządzeń

Kaspersky Security Center przypisze stan do każdego zarządzanego urządzenia. Określony stan zależy od tego, czy spełnione są warunki zdefiniowane przez użytkownika. W niektórych przypadkach, podczas przypisywania stanu do urządzenia, Kaspersky Security Center bierze pod uwagę flagę widoczności urządzenia w sieci (patrz tabela poniżej). Jeśli Kaspersky Security Center nie znajdzie urządzenia w sieci w ciągu dwóch godzin, flaga widoczności urządzenia zostanie ustawiona na *Nie jest widoczne*.

Stany są następujące:

- *Krytyczny* lub *Krytyczny / Widoczne*
- *Ostrzeżenie* lub *Ostrzeżenie / Widoczne*
- *OK* lub *OK / Widoczne*

Poniższa tabela wyświetla domyślne warunki, które muszą być spełnione, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia, wraz ze wszystkimi możliwymi wartościami.

Warunki przypisania stanu do urządzenia

Warunek	Opis warunku	Dostępne wartości
Aplikacja zabezpieczająca nie jest zainstalowana	Agent sieciowy jest zainstalowany na urządzeniu, ale aplikacja zabezpieczająca nie jest zainstalowana.	• Przycisk przełącznika jest ustawiony w pozycji włączenia. • Przycisk przełącznika jest ustawiony w pozycji wyłączenia.
Wykryto zbyt wiele wirusów	Niektóre wirusy zostały wykryte na urządzeniu przez zadanie wykrywania wirusów, na przykład, zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* oraz liczba wykrytych wirusów przekraczają określoną wartość.	Większe niż 0.
Poziom ochrony w czasie	Urządzenie jest widoczne w sieci, ale poziom ochrony w czasie rzeczywistym różni się od poziomu ustawionego (w warunku) przez	• Zatrzymane.

rzeczywistym jest inny niż poziom zdefiniowany przez administratora	administratora dla stanu urządzenia.	• Wstrzymane. • Uruchomione.
Skanowanie w poszukiwaniu złośliwego oprogramowania nie było wykonywane od dłuższego czasu	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale zadanie *Skanowanie w poszukiwaniu złośliwego oprogramowania* nie było uruchamiane w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego 7 dni temu lub wcześniej.	Więcej niż 1 dzień.
Bazy danych są nieaktualne	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale antywirusowe bazy danych nie były aktualizowane na tym urządzeniu w określonym przedziale czasu. Warunek jest stosowany tylko do urządzeń, które zostały dodane do bazy danych Serwera administracyjnego dzień wcześniej lub jeszcze wcześniej.	Więcej niż 1 dzień.
Niepołączony od dłuższego czasu	Agent sieciowy jest zainstalowany na urządzeniu, ale urządzenie nie było połączone z Serwerem administracyjnym w określonym przedziale czasu, ponieważ urządzenie było wyłączone.	Więcej niż 1 dzień.
Wykryto aktywne zagrożenia	Liczba nieprzetworzonych obiektów w folderze **Aktywne zagrożenia** przekracza określoną wartość.	Więcej niż 0 elementów.
Wymagane jest ponowne uruchomienie	Urządzenie jest widoczne w sieci, ale aplikacja wymaga ponownego uruchomienia urządzenia dłużej niż określony przedział czasu i z jednego z wybranych powodów.	Więcej niż 0 minut.
Zainstalowane są niekompatybilne aplikacje	Urządzenie jest widoczne w sieci, ale inwentaryzacja oprogramowania wykonywana poprzez Agenta sieciowego wykryła niekompatybilne aplikacje zainstalowane na urządzeniu.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto luki w oprogramowaniu	Urządzenie jest widoczne w sieci, a Agent sieciowy jest zainstalowany na urządzeniu, ale zadanie *Wyszukiwania luk i wymaganych aktualizacji* wykryło luki z określonym priorytetem w aplikacjach zainstalowanych na urządzeniu.	• Krytyczny. • Wysoki. • Średni. • Ignoruj, jeśli luka nie może być naprawiona. • Ignoruj, jeśli aktualizacja jest przypisana do instalacji.

Licencja utraciła ważność	Urządzenie jest widoczne w sieci, ale licencja utraciła ważność.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Licencja wkrótce utraci ważność	Urządzenie jest widoczne w sieci, ale licencja utraci ważność na urządzeniu za mniej niż określona liczba dni.	Więcej niż 0 dni.
Wyszukiwanie aktualizacji Windows Update nie było przeprowadzane od dłuższego czasu	Urządzenie jest widoczne w sieci, ale zadanie *Wykonaj synchronizację Windows Update* nie było uruchamiane w zdefiniowanym przedziale czasu.	Więcej niż 1 dzień.
Nieprawidłowy stan szyfrowania	Agent sieciowy jest zainstalowany na urządzeniu, ale wynik szyfrowania urządzenia jest równy określonej wartości.	• Nie zgadza się z zasadą w wyniku odmowy użytkownika (tylko dla urządzeń zewnętrznych). • Nie zgadza się z zasadą w wyniku błędu. • Po zastosowaniu zasady wymagane jest ponowne uruchomienie. • Nie określono zasady szyfrowania. • Nieobsługiwany. • Po zastosowaniu zasady.
Ustawienia urządzenia	Ustawienia urządzenia mobilnego są inne niż ustawienia, które zostały określone w zasadzie Kaspersky Endpoint Security for Android podczas sprawdzania reguł zgodności.	• Przycisk przełącznika

mobilnego nie są zgodne z zasadą		jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Wykryto nieprzetworzone incydenty	Nieprzetworzone zdarzenia zostały wykryte na urządzeniu. Zdarzenia mogą być tworzone automatycznie poprzez zarządzane aplikacje firmy Kaspersky zainstalowane na urządzeniu klienckim, a także ręcznie przez administratora.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Stan urządzenia zdefiniowany przez aplikację	Stan urządzenia jest definiowany przez zarządzaną aplikację.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Brakuje miejsca na dysku urządzenia	Wolnego miejsca na dysku jest mniej niż określona wartość lub urządzenie nie mogło zostać zsynchronizowane z Serwerem administracyjnym. Stan *Krytyczny* lub *Ostrzeżenie* zmieniło się na stan *OK*, gdy urządzenie zostało pomyślnie zsynchronizowane z Serwerem administracyjnym, a wolna przestrzeń na urządzeniu jest większa niż lub równa określonej wartości.	Więcej niż 0 MB.
Zarządzanie urządzeniem nie jest możliwe	Podczas wykrywania urządzeń, urządzenie zostało rozpoznane jako widoczne w sieci, ale więcej niż trzy próby synchronizacji z Serwerem administracyjnym nie powiodły się.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.
Ochrona jest wyłączona	Urządzenie jest widoczne w sieci, ale aplikacja zabezpieczająca na urządzeniu została wyłączona na dłużej niż określony przedział	Więcej niż 0 minut.

	czasu.	
Aplikacja zabezpieczająca nie jest uruchomiona	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale nie jest uruchomiona.	• Przycisk przełącznika jest ustawiony w pozycji wyłączenia. • Przycisk przełącznika jest ustawiony w pozycji włączenia.

Kaspersky Security Center umożliwia skonfigurowanie automatycznego przełączania stanu urządzenia w grupie administracyjnej, gdy spełnione są określone warunki. Jeśli określone warunki są spełnione, do urządzenia klienckiego zostanie przypisany jeden z następujących stanów: *Krytyczny* lub *Ostrzeżenie*. Jeśli określone warunki zostaną spełnione, urządzeniu klienckiemu zostanie przypisany stan *OK*.

Różne stany mogą odpowiadać różnym wartościom jednego warunku. Na przykład, domyślnie, jeśli warunek **Bazy danych są nieaktualne** posiada wartość **Ponad 3 dni**, do urządzenia klienckiego zostaje przypisany stan *Ostrzeżenie*; jeśli wartość to **Ponad 7 dni**, wówczas zostanie przypisany stan *Krytyczny*.

Jeśli aktualizujesz Kaspersky Security Center z poprzedniej wersji, wartości warunku **Bazy danych są nieaktualne** dla przypisania stanu do *Krytyczne* lub *Ostrzeżenie* nie zmienią się.

Jeśli Kaspersky Security Center przypisze stan do urządzenia, dla niektórych warunków (patrz kolumna Opis warunku) brana jest pod uwagę flaga widoczności. Na przykład, jeśli do zarządzanego urządzenia został przypisany stan *Krytyczny*, ponieważ spełniony był warunek Bazy danych są nieaktualne, a później flaga widoczności została ustawiona dla urządzenia, wówczas do urządzenia zostanie przypisany stan *OK*.

Konfigurowanie przełączania stanów urządzeń

Możesz zmienić warunki, aby przypisać stan *Krytyczny* lub *Ostrzeżenie* do urządzenia.

W celu włączenia zmiany stanu urządzenia na Krytyczny:

1. W menu głównym przejdź do **Urządzenia** → **Hierarchia grup**.
2. Na otwartej liście grup kliknij odnośnik z nazwą grupy, dla której chcesz zmienić przełączanie stanów urządzeń.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Krytyczny**.
5. W prawej części okna, w sekcji **Ustaw stan Krytyczny, jeśli** włącz warunek, aby przełączyć urządzenie do stanu *Krytyczny*.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.

7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.
8. Dla wybranego warunku ustaw żądaną wartość.
   Nie dla każdego warunku można ustawić wartości.
9. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Krytyczne*.

W celu włączenia zmiany stanu urządzenia na Ostrzeżenie:

1. W menu głównym przejdź do **Urządzenia** → **Hierarchia grup**.
2. Na otwartej liście grup kliknij odnośnik z nazwą grupy, dla której chcesz zmienić przełączanie stanów urządzeń.
3. W otwartym oknie właściwości wybierz zakładkę **Stan urządzenia**.
4. W lewej części okna wybierz **Ostrzeżenie**.
5. W prawej części okna, w sekcji **Ustaw stan Ostrzeżenie, jeśli** włącz warunek, aby przełączyć urządzenie do stanu *Ostrzeżenie*.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

6. Wybierz przycisk radiowy obok warunku na liście.
7. W lewym górnym rogu listy kliknij przycisk **Edytuj**.
8. Dla wybranego warunku ustaw żądaną wartość.
   Nie dla każdego warunku można ustawić wartości.
9. Kliknij **OK**.

Jeśli określone warunki zostaną spełnione, zarządzanemu urządzeniu zostanie przypisany stan *Ostrzeżenie*.

Konfigurowanie dostarczania powiadomień

Możesz skonfigurować powiadomienie o zdarzeniach występujących w Kaspersky Security Center. W zależności od wybranej metody powiadamiania, dostępne są następujące typy powiadomień:

- E-mail—Po wystąpieniu zdarzenia, Kaspersky Security Center wyśle powiadomienie na określone adresy e-mail.
- SMS—Po wystąpieniu zdarzenia, Kaspersky Security Center wyśle powiadomienie na określone numery telefonu.
- Plik wykonywalny—Po wystąpieniu zdarzenia, plik wykonywalny jest uruchamiany na Serwerze administracyjnym.

W celu skonfigurowania dostarczania powiadomień o zdarzeniach występujących w Kaspersky Security Center:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

Okno właściwości Serwera administracyjnego zostanie otwarte na zakładce **Ogólne**.

2. Kliknij sekcję **Powiadomienie** i w prawej części okna wybierz zakładkę dla metody powiadamiania, którą chcesz:

   - **E-mail**

Na zakładce **E-mail** można skonfigurować wysyłanie powiadomień o zdarzeniach za pośrednictwem poczty elektronicznej.

W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami.

W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX**, możesz użyć kilku wpisów MX adresów IP dla tej samej nazwy DNS serwera SMTP. Ta sama nazwa DNS może posiadać kilka wpisów MX z różnymi wartościami priorytetu odbierania wiadomości e-mail. Serwer administracyjny spróbuje wysłać powiadomienia e-mail do serwera SMTP w kolejności rosnącej priorytetów wpisów MX.

Jeśli włączysz opcję **Użyj przeszukiwania DNS MX** i nie włączysz korzystania z ustawień TLS, zalecane jest użycie ustawień DNSSEC na urządzeniu serwerowym jako dodatkowego środka ochrony wysyłania powiadomień e-mail.

Jeśli włączysz opcję **Użyj uwierzytelniania ESMTP**, możesz określić ustawienia uwierzytelniania ESMTP w polach **Nazwa użytkownika** i **Hasło**. Domyślnie, opcja ta jest wyłączona, a ustawienia uwierzytelniania ESMTP są niedostępne.

Możesz określić ustawienia TLS połączenia z serwerem SMTP:

- **Nie używaj TLS**

Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.

- **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

- **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**

Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić certyfikat dla połączenia TLS, klikając odnośnik **Określ certyfikaty**:

- Odszukaj plik certyfikatu serwera SMTP:

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

- Odszukaj plik certyfikatu klienta:

Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

- Certyfikat X-509:

Musisz określić plik z certyfikatem oraz plik z kluczem prywatnym. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po załadowaniu obu plików należy określić hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- Kontener pkcs12:

Musisz przesłać pojedynczy plik zawierający certyfikat i jego klucz prywatny. Po załadowaniu pliku należy podać hasło do dekodowania klucza prywatnego. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

W polu **Temat** wprowadź temat wiadomości e-mail. Możesz zostawić to pole puste.

Z listy rozwijalnej **Wybierz szablon** wybierz szablon tematu. Zmienna określona przez wybrany szablon zostanie automatycznie umieszczona w polu **Temat**. Możesz utworzyć temat wiadomości, wybierając kilka szablonów tematu.

W oknie **Adres e-mail nadawcy: Jeśli to ustawienie nie jest określone, użyty zostanie adres odbiorcy. Uwaga: Nie zalecamy używania adresu e-mail, który nie istnieje** określ adres e-mail nadawcy. Jeśli pozostawisz to pole puste, domyślnie użyty zostanie adres odbiorcy. Nie jest zalecane użycie adresu e-mail, który nie istnieje.

Pole **Treść powiadomienia** zawiera standardowy tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera dodatkowe parametry, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny. Istnieje możliwość zmodyfikowania treści wiadomości poprzez dodanie innych parametrów zastępczych z bardziej szczegółowymi danymi dotyczącymi zdarzenia.

> Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%”.

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Przycisk **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie na wskazany adres e-mail.

- SMS

Na zakładce **SMS** możesz skonfigurować wysyłanie powiadomień SMS o różnych zdarzeniach na telefon komórkowy. Wiadomości SMS są wysyłane poprzez bramkę pocztową.

W polu **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- Nazwa sieciowa Windows (nazwa NetBIOS) urządzenia
- Nazwa DNS serwera SMTP

W polu **Port serwera SMTP** określ numer portu komunikacji serwera SMTP. Domyślny numer portu to 25.

Jeśli opcja **Użyj uwierzytelniania ESMTP** jest włączona, możesz określić ustawienia uwierzytelniania ESMTP w polach **Nazwa użytkownika** i **Hasło**. Domyślnie, opcja ta jest wyłączona, a ustawienia uwierzytelniania ESMTP są niedostępne.

Możesz określić ustawienia TLS połączenia z serwerem SMTP:

- **Nie używaj TLS**

Możesz wybrać tę opcję, jeśli chcesz wyłączyć szyfrowanie wiadomości e-mail.

- **Użyj TLS, jeśli jest obsługiwany przez serwer SMTP**

Możesz wybrać tę opcję, jeśli chcesz korzystać z połączenia TLS z serwerem SMTP. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nawiąże połączenie z serwerem SMTP bez korzystania z TLS.

- **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**

Możesz wybrać tę opcję, jeśli chcesz korzystać z ustawień uwierzytelniania TLS. Jeśli serwer SMTP nie obsługuje TLS, Serwer administracyjny nie może nawiązać połączenia z serwerem SMTP.

Zalecane jest użycie tej opcji dla lepszej ochrony połączenia z serwerem SMTP. Jeśli wybierzesz tę opcję, możesz skonfigurować ustawienia uwierzytelniania dla połączenia TLS.

Jeśli wybierzesz wartość **Zawsze używaj TLS, sprawdź ważność certyfikatu serwera**, możesz określić certyfikat do uwierzytelniania serwera SMTP i wybrać, czy chcesz włączyć komunikację za pośrednictwem dowolnej wersji TLS, czy tylko za pośrednictwem TLS 1.2 lub nowszych wersji. Możesz także określić certyfikat do uwierzytelniania klienta na serwerze SMTP.

Możesz określić plik certyfikatu serwera SMTP, klikając odnośnik **Określ certyfikaty**:

Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji i przesłać go do Serwera administracyjnego. Kaspersky Security Center sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center nie może nawiązać połączenia z serwerem SMTP, jeśli certyfikat serwera SMTP nie zostanie odebrany z zaufanych urzędów certyfikacji.

W polu **Adresaci (adresy e-mail)** określ adresy e-mail, na jaki aplikacja będzie wysyłać powiadomienia. W tym polu możesz określić kilka adresów, oddzielając je średnikami. Powiadomienia będą dostarczane na numery telefonów skojarzone z określonymi adresami e-mail.

W polu **Temat** wprowadź temat wiadomości e-mail.

Z listy rozwijalnej **Wybierz szablon** wybierz szablon tematu. Zgodnie z wybranym szablonem zmienna zostanie umieszczona w polu **Temat**. Możesz utworzyć temat wiadomości, wybierając kilka szablonów tematu.

W oknie **Adres e-mail nadawcy:Jeśli to ustawienie nie jest określone, użyty zostanie adres odbiorcy. Uwaga: Nie zalecamy używania adresu e-mail, który nie istnieje** określ adres e-mail nadawcy. Jeśli pozostawisz to pole puste, domyślnie użyty zostanie adres odbiorcy. Nie jest zalecane użycie adresu e-mail, który nie istnieje.

W polu **Numery telefonów odbiorców wiadomości SMS** określ numery telefonów komórkowych odbiorców powiadomień SMS.

W polu **Treść powiadomienia** określ tekst z informacjami dotyczącymi zdarzenia, który aplikacja wysyła po wystąpieniu zdarzenia. Ten tekst zawiera parametry zastępcze, takie jak: nazwa zdarzenia, nazwa urządzenia oraz nazwa domeny.

Jeżeli tekst powiadomienia zawiera znak procentu (%), należy wpisać go dwa razy z rzędu, aby umożliwić wysyłanie wiadomości. Na przykład, „obciążenie procesora wynosi 100%%".

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

Kliknięcie **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie do określonego odbiorcy.

- **Plik wykonywalny do uruchomienia**

  Jeśli wybrana jest ta metoda powiadamiania, w polu wejściowym określ aplikację, która zostanie uruchomiona, gdy wystąpi zdarzenie.

  W polu **Plik wykonywalny, który będzie uruchamiany na Serwerze administracyjnym w momencie wystąpienia zdarzenia** określ folder i nazwę pliku, który ma zostać uruchomiony. Przed określeniem pliku przygotuj plik i określ symbole zastępcze, które definiują szczegóły zdarzeń, które mają zostać wysłane w treści powiadomienia. Folder i plik, który określasz, muszą znajdować się na Serwerze administracyjnym.

  Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

3. Na zakładce zdefiniuj ustawienia powiadamiania.
4. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.

Zapisane ustawienia dostarczania powiadomień zostaną zastosowane do wszystkich zdarzeń, które występują w Kaspersky Security Center.

Możesz zastąpić ustawienia dostarczania powiadomień dla pewnych zdarzeń w sekcji **Konfiguracja zdarzenia** ustawień Serwera administracyjnego, ustawień zasady lub ustawień aplikacji.

Wyświetlanie powiadomień o zdarzeniach po uruchomieniu pliku wykonywalnego

Kaspersky Security Center może powiadamiać administratora o zdarzeniach na urządzeniach klienckich poprzez uruchomienie pliku wykonywalnego. Plik wykonywalny musi zawierać inny plik wykonywalny z symbolami zastępczymi zdarzenia przekazywanymi administratorowi.

Symbole zastępcze opisujące zdarzenie

Symbol zastępczy	Opis symbolu zastępczego
%SEVERITY%	Priorytet zdarzenia
%COMPUTER%	Nazwa urządzenia, na którym wystąpiło zdarzenie

%DOMAIN%	Domena
%EVENT%	Zdarzenie
%DESCR%	Opis zdarzenia
%RISE_TIME%	Czas wystąpienia zdarzenia
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nazwa zadania
%KL_PRODUCT%	Agent sieciowy Kaspersky Security Center
%KL_VERSION%	Numer wersji Agenta sieciowego
%HOST_IP%	Adres IP
%HOST_CONN_IP%	Adres IP połączenia.

Na przykład:
Powiadomienia o zdarzeniach są wysyłane przez plik wykonywalny (na przykład script1.bat), w którym uruchomiony jest inny plik wykonywalny (na przykład script2.bat) z symbolem zastępczym %COMPUTER%. Po wystąpieniu zdarzenia, plik script1.bat jest uruchamiany na urządzeniu administratora, który uruchamia plik script2.bat z symbolem zastępczym %COMPUTER%. Administrator uzyska nazwę urządzenia, na którym wystąpiło zdarzenie.

Ogłoszenia firmy Kaspersky

W tej sekcji opisano, jak używać, konfigurować i wyłączać ogłoszenia Kaspersky.

Informacje o ogłoszeniach firmy Kaspersky

Sekcja Zapowiedzi firmy Kaspersky (**Monitorowanie i raportowanie** → **Zapowiedzi firmy Kaspersky**) zawiera informacje dotyczące Twojej wersji Kaspersky Security Center i zarządzanych aplikacji, zainstalowanych na zarządzanych urządzeniach. Kaspersky Security Center okresowo aktualizuje informacje w sekcji, usuwając nieaktualne ogłoszenia i dodając nowe informacje.

Kaspersky Security Center wyświetla tylko te ogłoszenia Kaspersky, które odnoszą się do aktualnie podłączonego Serwera administracyjnego i aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach tego Serwera administracyjnego. Ogłoszenia są wyświetlane indywidualnie dla dowolnego typu Serwera administracyjnego — głównego, podrzędnego lub wirtualnego.

Serwer administracyjny musi mieć połączenie z internetem, aby otrzymywać ogłoszenia Kaspersky.

Ogłoszenia zawierają informacje następujących typów:

- Ogłoszenia związane z bezpieczeństwem

  Ogłoszenia związane z bezpieczeństwem mają na celu zapewnienie aktualności i pełnej funkcjonalności aplikacji Kaspersky zainstalowanych w Twojej sieci. Ogłoszenia mogą zawierać informacje o krytycznych aktualizacjach aplikacji Kaspersky, poprawkach znalezionych luk w zabezpieczeniach i sposobach rozwiązania innych problemów w aplikacjach Kaspersky. Ogłoszenia związane z bezpieczeństwem są domyślnie włączone. Jeśli nie chcesz otrzymywać ogłoszeń, możesz wyłącz tę funkcję.

Aby wyświetlić informacje odpowiadające konfiguracji ochrony sieci, Kaspersky Security Center wysyła dane do serwerów Kaspersky w chmurze i odbiera tylko te powiadomienia, które odnoszą się do aplikacji Kaspersky zainstalowanych w Twojej sieci. Zestaw danych, które można wysłać do serwerów, opisano w Umowie licencyjnej użytkownika końcowego, którą akceptujesz podczas instalacji Serwera administracyjnego Kaspersky Security Center.

- Ogłoszenia marketingowe

  Ogłoszenia marketingowe obejmują informacje o specjalnych ofertach dla aplikacji Kaspersky, reklamach i nowościach od Kaspersky. Ogłoszenia marketingowe są domyślnie wyłączone. Otrzymujesz tego typu powiadomienia tylko wtedy, gdy włączyłeś Kaspersky Security Network (KSN). Możesz wyłączyć ogłoszenia marketingowe, wyłączając KSN.

  Aby wyświetlać tylko istotne informacje, które mogą być pomocne w ochronie urządzeń sieciowych i wykonywaniu codziennych zadań, Kaspersky Security Center wysyła dane do serwerów Kaspersky w chmurze i odbiera odpowiednie ogłoszenia. Zestaw danych, które można wysłać do serwerów, opisano w sekcji Przetwarzane dane w Oświadczeniu KSN.

Nowe informacje są podzielone na następujące kategorie według ważności:

1. Krytyczne informacje
2. Ważne wiadomości
3. Ostrzeżenie
4. Informacja

Jeśli w sekcji Ogłoszenia firmy Kaspersky pojawią się nowe informacje, konsola Kaspersky Security Center Web Console wyświetli etykietę powiadomienia odpowiadającą poziomowi ważności ogłoszeń. Możesz kliknąć etykietę, aby wyświetlić to ogłoszenie w sekcji Ogłoszenia firmy Kaspersky.

Możesz określić Ustawienia ogłoszeń firmy Kaspersky, w tym kategorie ogłoszeń, które chcesz przeglądać, i gdzie wyświetlać etykietę powiadomienia.

Określanie ustawień ogłoszeń Kaspersky

W sekcji Ogłoszenia firmy Kaspersky możesz określić ustawienia ogłoszeń firmy Kaspersky, w tym kategorie ogłoszeń, które chcesz przeglądać, i gdzie wyświetlać etykietę powiadomienia.

W celu skonfigurowania ogłoszeń Kaspersky:

1. W menu głównym przejdź do **Monitorowanie i raportowanie** → **Ogłoszenia Kaspersky**.
2. Kliknij odnośnik **Ustawienia**.

   Zostanie otwarte okno ustawień ogłoszeń Kaspersky.
3. Określ następujące ustawienia:

   - Wybierz poziom ważności ogłoszeń, które chcesz przejrzeć. Ogłoszenia z innych kategorii nie będą wyświetlane.
   - Wybierz, gdzie chcesz widzieć etykietę powiadomienia. Etykieta może być wyświetlana we wszystkich sekcjach konsoli lub w sekcji **Monitorowanie i raportowanie** i jego podsekcjach.

4. Kliknij przycisk **OK**.

   Zostaną określone ustawienia ogłoszeń firmy Kaspersky.

Wyłączanie ogłoszeń Kaspersky

Sekcja Ogłoszenia firmy Kaspersky (**Monitorowanie i raportowanie → Ogłoszenia firmy Kaspersky**) zawiera informacje dotyczące Twojej wersji Kaspersky Security Center i zarządzanych aplikacji, zainstalowanych na zarządzanych urządzeniach. Jeśli nie chcesz otrzymywać ogłoszeń firmy Kaspersky, możesz wyłączyć tę funkcję.

Ogłoszenia firmy Kaspersky obejmują dwa rodzaje informacji: ogłoszenia związane z bezpieczeństwem oraz ogłoszenia marketingowe. Możesz wyłączyć ogłoszenia każdego typu osobno.

W celu wyłączenia ogłoszeń związanych z bezpieczeństwem:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogłoszenia Kaspersky**.

3. Przełącz przycisk przełączania na pozycję **Ogłoszenia związane z bezpieczeństwem Wyłączono**.

4. Kliknij przycisk **Zapisz**.

   Ogłoszenia firmy Kaspersky są wyłączone.

Ogłoszenia marketingowe są domyślnie wyłączone. Otrzymujesz ogłoszenia marketingowe tylko wtedy, gdy włączyłeś Kaspersky Security Network (KSN). Możesz wyłączyć tego typu ogłoszenia, wyłączając KSN.

W celu wyłączenia ogłoszeń marketingowych:

1. W menu aplikacji kliknij ikonę ustawienia ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ustawienia KSN Proxy**.

3. Wyłącz opcję **Użyj Kaspersky Security Network Włączono**.

4. Kliknij przycisk **Zapisz**.

   Ogłoszenia marketingowe są wyłączone.

Przeglądanie informacji dotyczących wykrycia zagrożeń

Możesz włączyć lub wyłączyć wyświetlanie informacji o alertach.

*W celu włączenia lub wyłączenia sekcji **Alerty** w menu głównym:*

1. W menu głównym przejdź do ustawień konta i wybierz **Opcje interfejsu**.

2. W otwartym oknie **Opcje interfejsu** włącz lub wyłącz opcję **Pokaż alerty EDR**.

3. Kliknij **Zapisz**.

Konsola wyświetla podsekcję **Alerty** w sekcji **Monitorowanie i raportowanie** menu głównego. W podsekcji **Alerty** możesz przejrzeć informacje dotyczące wykrycia zagrożeń na urządzeniach końcowych. Jeśli dodasz klucz licencyjny dla EDR Optimum, wówczas Kaspersky Security Center Web Console automatycznie wyświetli podsekcję **Alerty** w sekcji **Monitorowanie i raportowanie** menu głównego. Dodatkowo, możesz dodać widżet, który wyświetla informacje o powiadomieniach. Dodatkowo, jeśli zainstalowałeś wtyczkę EDR Optimum, możesz przejrzeć szczegółowe informacje o wykrytych zagrożeniach, klikając odnośnik **więcej informacji**.

Rejestrowanie aktywności Kaspersky Security Center Web Console

Rejestrowanie aktywności Kaspersky Security Center Web Console może pomóc w zbadaniu przyczyny problemów z działaniem oprogramowania. Jeśli kontaktujesz się z działem pomocy technicznej Kaspersky w sprawie problemów z działaniem Kaspersky Security Center Web Console, specjaliści z działu pomocy technicznej Kaspersky mogą poprosić o pliki dziennika Kaspersky Security Center Web Console. Pliki dziennika Kaspersky Security Center Web Console są przechowywane w folderze <Folder instalacyjny Kaspersky Security Center Web Console>/logs przez cały czas korzystania z aplikacji. Pliki raportów nie są automatycznie wysyłane do specjalistów z pomocy technicznej Kaspersky.

W celu włączenia rejestrowania aktywności Kaspersky Security Center Web Console:

Zaznacz pole **Enable logging of Kaspersky Security Center 14 Web Console activities** w oknie **Kaspersky Security Center 14 Web Console connection settings** kreatora instalacji Kaspersky Security Center Web Console.

Pliki raportów są w formacie tekstowym.

Nazwy plików raportów są w formacie logs-<nazwa komponentu>.<nazwa urządzenia>-<numer rewizji pliku>.RRRR-MM-DD, gdzie:

- <nazwa składnika> to nazwa składnika Kaspersky Security Center lub nazwa wtyczki administracyjnej Kaspersky Security Center Web Console.
- <nazwa urządzenia> to nazwa urządzenia, na którym jest uruchomiony <nazwa komponentu>.
- <numer rewizji pliku> to numer pliku raportu, utworzonego dla komponentu <nazwa_komponentu>, który działa na hoście <nazwa urządzenia>. W ciągu dnia może zostać utworzonych kilka plików raportów dla tego samego komponentu <nazwa komponentu> i urządzenia <nazwa urządzenia>. Maksymalny rozmiar pliku raportu wynosi 50 megabajtów (MB). Jeśli zostanie osiągnięty maksymalny rozmiar pliku, zostanie utworzony nowy plik raportu. Nowy plik raportu <numer rewizji pliku> zostanie zwiększony o 1.
- RRRR, MM i DD to rok, miesiąc i dzień pierwszego utworzenia raportu. Gdy zacznie się nowy dzień, zostanie utworzony nowy plik raportu.

Integracja Kaspersky Security Center z innymi rozwiązaniami

W tej sekcji opisano, jak skonfigurować dostęp z Kaspersky Security Center Web Console do innej aplikacji Kaspersky, takiej jak Kaspersky Endpoint Detection and Response oraz Kaspersky Managed Detection and Response. Dodatkowo, ta sekcja opisuje sposób skonfigurowania eksportowania do systemów SIEM.

Konfigurowanie dostępu do KATA / KEDR Web Console

Kaspersky Anti Targeted Attack (KATA) i Kaspersky Endpoint Detection and Response (KEDR) to dwie funkcjonalne sekcje Kaspersky Anti Targeted Attack Platform. Możesz zarządzać tymi sekcjami funkcjonalnymi poprzez konsolę Web Console dla Kaspersky Anti Targeted Attack Platform (KATA / KEDR Web Console). Jeśli używasz Kaspersky Security Center Web Console i KATA / KEDR Web Console, możesz skonfigurować dostęp do KATA / KEDR Web Console bezpośrednio z poziomu interfejsu Kaspersky Security Center Web Console.

W celu skonfigurowania dostępu do KATA / KEDR Web Console:

1. W menu głównym przejdź do sekcji **Ustawienia konsoli** → **Integracja**.
2. Na zakładce **Integracja** wybierz sekcję **KATA**.
3. Wprowadź adres URL KATA / KEDR Web Console w polu **URL do KATA/KEDR Web Console**.
4. Kliknij przycisk **Zapisz**.

Lista rozwijalna **Zarządzanie zaawansowane** zostanie dodana do okna głównego aplikacji. Możesz użyć tego menu, aby otworzyć KATA / KEDR Web Console. Po kliknięciu **Zaawansowane cyberbezpieczeństwo**, w przeglądarce zostanie otwarta nowa zakładka z określonym adresem internetowym.

Nawiązywanie połączenia w tle

Aby umożliwić Kaspersky Security Center Web Console wykonywanie zadań w tle, musisz ustanowić połączenie w tle pomiędzy Kaspersky Security Center Web Console i Serwerem administracyjnym. Możesz nawiązać to połączenie tylko wtedy, jeśli Twoje konto ma uprawnienie **Modyfikuj listy ACL** obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika.**

Jeśli zainstalujesz wtyczkę Kaspersky Endpoint Security for Windows 12.0 lub zaktualizujesz wtyczkę Kaspersky Endpoint Security for Windows z wersji wcześniejszej niż 11.7, a połączenie w tle nie zostanie jeszcze nawiązane, zostanie wyświetlone powiadomienie, że musisz nawiązać połączenie w tle. Ponadto będziesz musiał nadać kontu usługi uprawnienia obszaru funkcjonalnego **Funkcje ogólne: Operacje na Serwerze administracyjnym**.

Aby nawiązać połączenie w tle:

1. W menu głównym przejdź do sekcji **Ustawienia konsoli** → **Integracja**.
2. Na karcie **Integracja** przełącz przełącznik służący do nawiązywania połączenia w tle do pozycji: **Nawiąż połączenie w tle na potrzeby integracji między usługami Włączono**.
3. W otwartej sekcji **Usługa, która nawiązuje połączenie w tle, zostanie uruchomiona na serwerze Kaspersky Security Center Web Console** kliknij przycisk **OK**.

Połączenie w tle pomiędzy konsolą Kaspersky Security Center Web Console i Serwerem administracyjnym jest nawiązywane. Serwer administracyjny tworzy konto dla połączenia w tle, które jest używane jako konto usługi do utrzymywania interakcji między Kaspersky Security Center a inną aplikacją lub rozwiązaniem Kaspersky. Nazwa tego konta usługi zawiera przedrostek NWCSvcUser.

Serwer administracyjny automatycznie zmienia hasło do konta usługi co 30 dni ze względów bezpieczeństwa. Nie możesz usunąć konta usługi ręcznie. Serwer administracyjny automatycznie usuwa to konto po wyłączeniu połączenia między usługami. Serwer administracyjny tworzy jedno konto usługi dla każdej Konsoli administracyjnej i przypisuje wszystkie konta usług do grupy bezpieczeństwa o nazwie ServiceNwcGroup. Serwer administracyjny tworzy grupę zabezpieczeń automatycznie podczas procesu instalacji Kaspersky Security Center. Nie możesz usunąć tej grupy zabezpieczeń ręcznie.

Eksportowanie zdarzeń do systemów SIEM

Ta sekcja opisuje sposób skonfigurowania eksportowania zdarzeń do systemów SIEM.

Scenariusz: Konfigurowanie eksportowania zdarzeń do systemów SIEM

Kaspersky Security Center umożliwia konfigurowanie przy użyciu jednej z następujących metod: eksportowanie do dowolnego systemu SIEM korzystającego z formatu Syslog, eksportowanie do systemów QRadar, Splunk, ArcSight SIEM korzystających z formatów LEEF i CEF lub eksportowanie zdarzeń do systemów SIEM bezpośrednio z bazy danych Kaspersky Security Center. Po zakończeniu tego scenariusza Serwer administracyjny automatycznie wysyła zdarzenia do systemu SIEM.

Wymagania wstępne

Zanim rozpoczniesz konfigurowanie eksportowania zdarzeń w Kaspersky Security Center:

- Dowiedz się więcej o metodach eksportowania zdarzeń.
- Upewnij się, że posiadasz wartości ustawień systemowych.

> Możesz wykonać kroki tego scenariusza w dowolnej kolejności.

Proces eksportowania zdarzeń do systemu SIEM obejmuje następujące kroki:

- **Konfigurowanie systemu SIEM do odbierania zdarzeń z Kaspersky Security Center**

  Instrukcja: Konfigurowanie eksportowania zdarzeń w systemie SIEM

- **Wybieranie zdarzeń, które chcesz wyeksportować do systemu SIEM:**

  Dostępne instrukcje:

  - Konsola administracyjna: Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog, Oznaczanie ogólnych zdarzeń do eksportowania w formacie Syslog
  - Kaspersky Security Center Web Console: Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog, Oznaczanie ogólnych zdarzeń do eksportowania w formacie Syslog

- **Konfigurowanie eksportowania zdarzeń do systemu SIEM za pomocą jednej z poniższych metod:**

  - Korzystanie z protokołów TCP/IP, UDP lub TLS przez protokoły TCP.

    Dostępne instrukcje:

- Konsola administracyjna: Konfigurowanie eksportowania zdarzeń do systemów SIEM
- Kaspersky Security Center Web Console: Konfigurowanie eksportowania zdarzeń do systemów SIEM

- Używanie eksportowania zdarzeń bezpośrednio z bazy danych Kaspersky Security Center (zestaw widoków publicznych jest dostępny w bazie danych Kaspersky Security Center; opis tych widoków publicznych można znaleźć w dokumencie klakdb.chm).

Wyniki

Po skonfigurowaniu eksportowania zdarzeń do systemu SIEM możesz przeglądać eksportowanie wyników, jeśli wybrałeś zdarzenia, które chcesz wyeksportować.

Czynności niezbędne do wykonania przed rozpoczęciem pracy

Podczas konfigurowania automatycznego eksportowania zdarzeń w Kaspersky Security Center musisz określić niektóre ustawienia systemu SIEM. Zalecane jest wcześniejsze sprawdzenie tych ustawień w celu przygotowania do konfiguracji Kaspersky Security Center.

W celu pomyślnego skonfigurowania automatycznego wysyłania zdarzeń do systemu SIEM należy znać następujące ustawienia:

- **Adres serwera systemu SIEM**

  Adres IP serwera, na którym zainstalowany jest aktualnie używany system SIEM. Sprawdź wartość tego ustawienia w ustawieniach systemu SIEM.

- **Port serwera systemu SIEM**

  Numer portu używanego do nawiązania połączenia pomiędzy Kaspersky Security Center a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

- **Protokół**

  Protokół używany do przesyłania wiadomości z Kaspersky Security Center do Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

Informacje o zdarzeniach w Kaspersky Security Center

Kaspersky Security Center umożliwia otrzymywanie informacji o zdarzeniach występujących podczas działania Serwera administracyjnego i aplikacji firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Informacje o zdarzeniach są zapisywane w bazie danych Serwera administracyjnego. Możesz wyeksportować te informacje do zewnętrznych systemów SIEM. Eksportowanie informacji o zdarzeniach do zewnętrznych systemów SIEM umożliwia administratorom systemów SIEM natychmiastowe reagowanie na zdarzenia dotyczące systemu bezpieczeństwa, które pojawiają się na zarządzanych urządzeniach lub w grupach administracyjnych.

Typy zdarzeń

W Kaspersky Security Center dostępne są następujące typy zdarzeń:

- Zdarzenia ogólne. Te zdarzenia występują we wszystkich zarządzanych aplikacjach firmy Kaspersky. Przykładem zdarzenia ogólnego jest Epidemia wirusa. Zdarzenia ogólne mają dokładnie zdefiniowaną składnię i semantykę. Zdarzenia ogólne są używane, na przykład, w raportach i pulpitach nawigacyjnych.
- Zarządzane zdarzenia charakterystyczne dla aplikacji firmy Kaspersky. Każda zarządzana aplikacja firmy Kaspersky posiada swój zestaw zdarzeń.

Źródła zdarzeń

Zdarzenia mogą być generowane przez następujące aplikacje:

- Składniki Kaspersky Security Center:
  - Serwer administracyjny
  - Agent sieciowy
  - Serwer iOS MDM
  - Serwer urządzeń mobilnych Exchange
- Zarządzane aplikacje Kaspersky

  Szczegółowe informacje na temat zdarzeń generowanych przez aplikacje zarządzane przez Kaspersky można znaleźć w dokumentacji odpowiedniej aplikacji.

Możesz wyświetlić pełną listę zdarzeń, które mogą być generowane przez aplikację na karcie **Konfiguracja zdarzenia** w zasadzie aplikacji. W przypadku Serwera administracyjnego możesz dodatkowo wyświetlić listę zdarzeń we właściwościach Serwera administracyjnego.

Poziom ważności zdarzeń

Każde zdarzenie posiada priorytet. W zależności od warunków wystąpienia zdarzenia, może ono posiadać różne priorytety. Istnieją cztery priorytety zdarzeń:

- *Zdarzenie krytyczne* to zdarzenie, które wskazuje wystąpienie krytycznego problemu mogącego prowadzić do utraty danych, problemów z działaniem lub błędu krytycznego.
- *Błąd funkcjonalny* to zdarzenie, które wskazuje poważny problem, błąd lub problem z działaniem, który wystąpił podczas działania aplikacji lub podczas przeprowadzania procedury.
- *Ostrzeżenie* to zdarzenie, które niekoniecznie jest poważne, ale wskazuje możliwość wystąpienia potencjalnego problemu w przyszłości. Większość zdarzeń otrzymuje priorytet „Ostrzeżenie", jeśli aplikacja może zostać przywrócona bez utraty danych lub możliwości funkcyjnych aplikacji.
- *Informacja* to zdarzenie, którego celem jest informowanie o pomyślnym zakończeniu działania, właściwym funkcjonowaniu aplikacji lub zakończeniu procedury.

Każde zdarzenie posiada zdefiniowany okres przechowywania, w trakcie którego możesz przejrzeć lub zmodyfikować to zdarzenie w Kaspersky Security Center. Niektóre zdarzenia nie są domyślnie zapisywane w bazie danych Serwera administracyjnego, ponieważ ich zdefiniowany okres przechowywania wynosi zero. Tylko te zdarzenia, które będą przechowywane w bazie danych Serwera administracyjnego przynajmniej jeden dzień, mogą zostać wyeksportowane do systemów zewnętrznych.

Informacje o eksportowaniu zdarzeń

Eksportowanie zdarzeń może być używane w obrębie scentralizowanych systemów, które zajmują się problemami z bezpieczeństwem na poziomie organizacyjnym i technicznym, zapewniają usługi monitorowania ochrony oraz skonsolidowane informacje z różnych rozwiązań. To są systemy SIEM, które oferują przeprowadzania w czasie rzeczywistym analizy ostrzeżeń i zdarzeń zabezpieczeń, wygenerowanych przez aplikacje i sprzęt w sieci, lub Security Operation Centers (SOCs).

Te systemy otrzymują dane z wielu źródeł, w tym sieci, ochrony, serwerów, baz danych i aplikacji. Systemy SIEM oferują także funkcjonalność konsolidowania monitorowanych danych, aby pomóc w uniknięciu przeoczenia zdarzeń krytycznych. Dodatkowo, systemy przeprowadzają zautomatyzowaną analizę powiązanych zdarzeń i ostrzeżeń w celu powiadomienia administratorów o nagłych problemach z bezpieczeństwem. Wysyłanie ostrzeżeń może zostać zaimplementowane poprzez pulpit nawigacyjny lub wysyłanie ostrzeżeń może się odbywać poprzez kanały firm trzecich, na przykład pocztę elektroniczną.

Proces eksportowania zdarzeń z Kaspersky Security Center do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia – Kaspersky Security Center oraz odbiorca zdarzenia – system SIEM. Aby pomyślnie eksportować zdarzenia, należy skonfigurować tę funkcję w posiadanym systemie SIEM i w Konsoli administracyjnej Kaspersky Security Center. Nie ma znaczenia, która strona zostanie skonfigurowana jako pierwsza. Możesz skonfigurować przesyłanie zdarzeń w Kaspersky Security Center, a następnie skonfigurować odbieranie zdarzeń przez system SIEM lub na odwrót.

Metody wysyłania zdarzeń z Kaspersky Security Center

Dostępne są trzy metody wysyłania zdarzeń z Kaspersky Security Center do systemów zewnętrznych:

- Wysyłanie zdarzeń po protokole Syslog do dowolnego systemu SIEM

  Korzystając z protokołu Syslog, możesz przekazywać dowolne zdarzenia, które wystąpiły na Serwerze administracyjnym Kaspersky Security Center i w aplikacjach firmy Kaspersky zainstalowanych na zarządzanych urządzeniach. Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Możesz go użyć do eksportowania zdarzeń do systemu SIEM.

  W tym celu należy zaznaczyć zdarzenia, które chcemy przekazać do systemu SIEM. Możesz zaznaczyć zdarzenia w Konsoli administracyjnej lub konsoli Kaspersky Security Center Web Console. Tylko zaznaczone zdarzenia będą przekazywane do systemu SIEM. Jeśli nic nie zaznaczysz, żadne zdarzenia nie zostaną przekazane.

- Wysyłanie zdarzeń po protokołach CEF i LEEF do systemów QRadar, Splunk i ArcSight

  Możesz używać protokołów CEF i LEEF do eksportowania zdarzeń ogólnych. Podczas eksportowania zdarzeń po protokołach CEF i LEEF nie masz możliwości wyboru określonych zdarzeń do wyeksportowania. Eksportowane są wszystkie zdarzenia ogólne. W przeciwieństwie do protokołu Syslog, protokoły CEF i LEEF nie są uniwersalne. Protokoły CEF i LEEF są przeznaczone dla odpowiednich systemów SIEM (QRadar, Splunk i ArcSight). Dlatego też, jeśli wybierzesz eksportowanie zdarzeń poprzez jeden z tych protokołów, użyjesz parsera w systemie SIEM.

Aby wyeksportować zdarzenia poprzez protokoły CEF i LEEF, funkcja integracji z systemami SIEM musi być aktywowana w Serwerze administracyjnym przy użyciu aktywnego klucza licencyjnego lub ważnego kodu aktywacyjnego.

- Bezpośrednio z bazy danych Kaspersky Security Center do dowolnego systemu SIEM

  Ta metoda eksportowania zdarzeń może zostać użyta do odbierania zdarzeń bezpośrednio z widoków publicznych bazy danych przy użyciu zapytań SQL. Wyniki zapytań są zapisywane do pliku XML, który może zostać użyty jako dane wejściowe systemu zewnętrznego. Tylko zdarzenia dostępne w widokach publicznych mogą być eksportowane bezpośrednio z bazy danych.

Odbieranie zdarzeń przez system SIEM

System SIEM musi odbierać i poprawnie analizować zdarzenia otrzymywane z Kaspersky Security Center. W tym celu należy odpowiednio skonfigurować system SIEM. Konfiguracja zależy od specyfiki używanego systemu SIEM. Jednakże istnieje kilka ogólnych kroków w konfiguracji wszystkich systemów SIEM, takie jak konfigurowanie odbiorcy i analizatora.

Informacje o konfigurowaniu eksportowania zdarzeń w systemie SIEM

Proces eksportowania zdarzeń z Kaspersky Security Center do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia—Kaspersky Security Center oraz odbiorca zdarzenia—system SIEM. Należy skonfigurować eksportowanie zdarzeń w posiadanym systemie SIEM i w Kaspersky Security Center.

Ustawienia określane w systemie SIEM zależą od określonego systemu, którego używasz. Zazwyczaj dla wszystkich systemów SIEM należy skonfigurować odbiorcę i, opcjonalnie, analizatora wiadomości do analizowania otrzymanych zdarzeń.

Konfigurowanie odbiorcy

Aby otrzymywać zdarzenia wysyłane przez Kaspersky Security Center, należy skonfigurować odbiorcę w swoim systemie SIEM. W systemie SIEM powinny zostać określone następujące ustawienia:

- **Protokół eksportu lub typ wejścia**

  Jest to protokół obsługujący przesyłanie wiadomości - TCP/IP lub UDP. Ten protokół musi być taki sam, jak protokół, który określiłeś w Kaspersky Security Center.

- **Port**

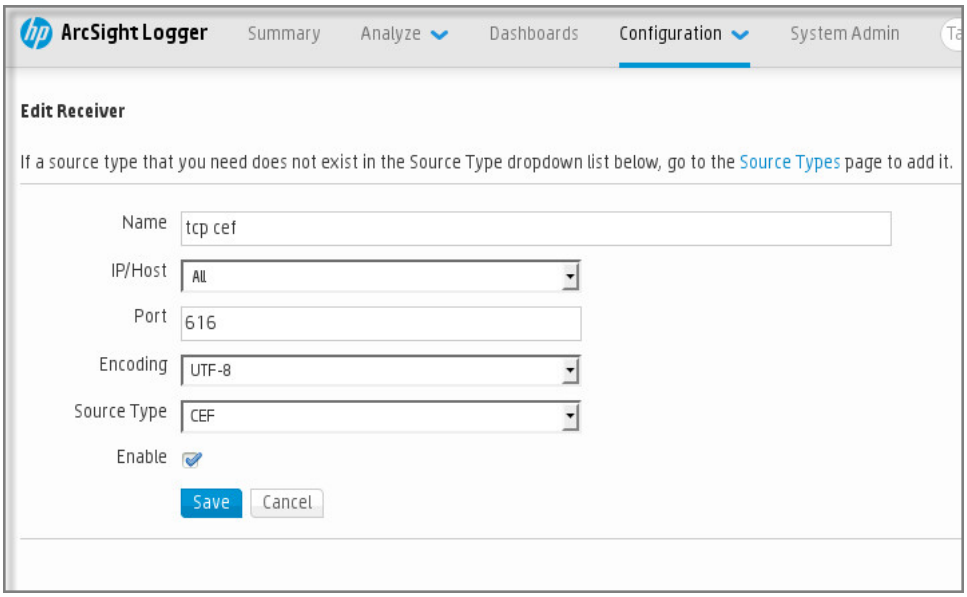
  Numer portu do nawiązana połączenia z Kaspersky Security Center. Ten port musi być taki sam, jak port, który określiłeś w Kaspersky Security Center.

- **Protokół wiadomości lub typ źródła**

  Protokół używany do eksportowania zdarzeń do systemu SIEM. Może to być jeden ze standardowych protokołów: Syslog, CEF lub LEEF. System SIEM wybiera analizatora wiadomości zgodnie z protokołem, który określiłeś.

W zależności od używanego systemu SIEM, konieczne może być określenie niektórych dodatkowych ustawień odbiorcy.

Poniższy rysunek przedstawia okno konfiguracji odbiorcy w ArcSight.



Konfiguracja odbiorcy w ArcSight

Analizator wiadomości

Wyeksportowane zdarzenia są przekazywane do systemu SIEM jako wiadomości. Te wiadomości muszą być odpowiednio przeanalizowane, aby informacje na temat zdarzeń mogły być użyte przez system SIEM. Analizatory wiadomości są częścią systemu SIEM; są używane do podzielenia zawartości wiadomości na odpowiednie pola, takie jak: ID zdarzenia, priorytet, opis, parametry itd. Umożliwia to systemowi SIEM przetworzenie zdarzeń otrzymanych z Kaspersky Security Center tak, aby mogły być przechowywane w bazie danych systemu SIEM.

Każdy system SIEM posiada zestaw standardowych analizatorów wiadomości. Kaspersky także dostarcza analizatory wiadomości dla niektórych systemów SIEM, na przykład dla QRadar i ArcSight. Te analizatory wiadomości można pobrać ze stron internetowych odpowiednich systemów SIEM. Podczas konfigurowania odbiorcy możesz wybrać używanie jednego ze standardowych analizatorów wiadomości lub analizatora wiadomości od Kaspersky.

Oznaczenie zdarzeń do wyeksportowania do systemów SIEM w formacie Syslog

W tej sekcji opisano, jak oznaczyć zdarzenia do dalszego eksportu do systemów SIEM w formacie Syslog.

Informacje dotyczące oznaczania zdarzeń do wyeksportowania do systemu SIEM w formacie Syslog

Po włączeniu automatycznego eksportowania zdarzeń, należy wskazać zdarzenia, które zostaną wyeksportowane do zewnętrznego systemu SIEM.

Możesz skonfigurować eksportowanie zdarzeń w formacie Syslog do zewnętrznego systemu w oparciu o jeden z następujących warunków:

- Oznaczanie zdarzeń ogólnych. Jeśli zdarzenia do wyeksportowania oznaczysz w zasadzie, w ustawieniach zdarzenia lub w ustawieniach Serwera administracyjnego system SIEM otrzyma oznaczone zdarzenia, które wystąpiły we wszystkich aplikacjach zarządzanych przez określoną zasadę. Jeśli wyeksportowane zdarzenia były wybrane w profilu, nie będziesz mógł ich ponownie zdefiniować dla aplikacji zarządzanej przez ten profil.

- Oznaczanie zdarzeń dla zarządzanej aplikacji. Jeśli oznaczysz zdarzenia do wyeksportowania dla zarządzanej aplikacji, zainstalowanej na zarządzanym urządzeniu, system SIEM otrzyma tylko zdarzenia, które wystąpiły w tej aplikacji.

Oznaczanie zdarzeń aplikacji Kaspersky do eksportowania w formacie Syslog

Jeśli chcesz wyeksportować zdarzenia, które wystąpiły w określonej zarządzanej aplikacji, zainstalowanej na zarządzanych urządzeniach, w zasadzie aplikacji oznacz zdarzenia do wyeksportowania. W takim przypadku zaznaczone zdarzenia są eksportowane ze wszystkich urządzeń objętych zakresem zasady.

W celu oznaczenia zdarzeń do wyeksportowania dla określonej zarządzanej aplikacji:

1. W menu głównym przejdź do **Urządzenia** → **Profile zasad**.
2. Kliknij zasadę aplikacji, dla której chcesz oznaczyć zdarzenia.

   Zostanie otwarte okno ustawień zasady.
3. Przejdź do sekcji **Konfiguracja zdarzenia**.
4. Zaznacz pola obok zdarzeń, które chcesz wyeksportować do systemu SIEM.
5. Kliknij przycisk **Zaznacz do eksportu do systemu SIEM poprzez Syslog**.

   Możesz także oznaczyć zdarzenie do wyeksportowania do systemu SIEM w sekcji **Rejestracja zdarzenia**, która zostanie otwarta po kliknięciu odnośnika zdarzenia.
6. Znacznik (✓) pojawi się w kolumnie **Syslog** zdarzenia lub zdarzeń, które oznaczyłeś do wyeksportowania do systemu SIEM.
7. Kliknij przycisk **Zapisz**.

Oznaczone zdarzenia z zarządzanej aplikacji są gotowe do wyeksportowania do systemu SIEM.

Możesz zaznaczyć, które zdarzenia wyeksportować do systemu SIEM dla określonego zarządzanego urządzenia. Jeśli poprzednio wyeksportowane zdarzenia były oznaczone w zasadzie aplikacji, nie będziesz mógł ponownie zdefiniować oznaczonych zdarzeń dla zarządzanego urządzenia.

W celu oznaczenia zdarzeń do wyeksportowania dla zarządzanego urządzenia:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.

   Zostanie wyświetlona lista zarządzanych urządzeń.
2. Kliknij odnośnik z nazwą żądanego urządzenia na liście zarządzanych urządzeń.

   Zostanie wyświetlone okno właściwości wybranego urządzenia.
3. Przejdź do sekcji **Aplikacje**.

4. Kliknij odnośnik z nazwą żądanej aplikacji na liście aplikacji.

5. Przejdź do sekcji **Konfiguracja zdarzenia**.

6. Zaznacz pola obok zdarzeń, które chcesz wyeksportować do SIEM.

7. Kliknij przycisk **Zaznacz do eksportu do systemu SIEM poprzez Syslog**.

   Dodatkowo, możesz oznaczyć zdarzenie do wyeksportowania do systemu SIEM w sekcji **Rejestracja zdarzenia**, która zostanie otwarta po kliknięciu odnośnika zdarzenia.

8. Znacznik (✓) pojawi się w kolumnie **Syslog** zdarzenia lub zdarzeń, które oznaczyłeś do wyeksportowania do systemu SIEM.

Od tego momentu Serwer administracyjny wysyła do systemu SIEM oznaczone zdarzenia, jeśli eksportowanie do systemu SIEM zostało skonfigurowane.

Oznaczanie ogólnych zdarzeń do eksportu w formacie Syslog

Możesz oznaczyć zdarzenia ogólne, które Serwer administracyjny wyeksportuje do systemów SIEM przy użyciu formatu Syslog.

W celu oznaczenia zdarzeń ogólnych do wyeksportowania do systemu SIEM:

1. Wykonaj jedną z poniższych czynności:

   - W menu aplikacji kliknij ikonę ustawienia (⚙) obok nazwy żądanego Serwera administracyjnego.
   - W menu głównym przejdź do **Urządzenia** → **Profile zasad**, a następnie kliknij odnośnik do zasady.

2. W otwartym oknie przejdź na zakładkę **Konfiguracja zdarzenia**.

3. Kliknij **Zaznacz do eksportu do systemu SIEM poprzez Syslog**.

   Dodatkowo, możesz oznaczyć zdarzenie do wyeksportowania do systemu SIEM w sekcji **Rejestracja zdarzenia**, która zostanie otwarta po kliknięciu odnośnika zdarzenia.

4. Znacznik (✓) pojawi się w kolumnie **Syslog** zdarzenia lub zdarzeń, które oznaczyłeś do wyeksportowania do systemu SIEM.

Od tego momentu Serwer administracyjny wysyła do systemu SIEM oznaczone zdarzenia, jeśli eksportowanie do systemu SIEM zostało skonfigurowane.

Informacje dotyczące eksportowania zdarzeń przy użyciu formatów CEF i LEEF

Możesz użyć formatów CEF i LEEF, aby wyeksportować ogólne zdarzenia do systemów SIEM, a także zdarzenia przesyłane przez aplikacje Kaspersky do Serwera administracyjnego. Zestaw eksportowanych zdarzeń jest predefiniowany i nie możesz wybrać zdarzeń do wyeksportowania.

Aby wyeksportować zdarzenia poprzez protokoły CEF i LEEF, funkcja integracji z systemami SIEM musi być aktywowana w Serwerze administracyjnym przy użyciu aktywnego klucza licencyjnego lub ważnego kodu aktywacyjnego.

Wybierz format eksportowania w oparciu o używany system SIEM. Poniższa tabela wyświetla systemy SIEM i odpowiadające im formaty eksportu.

Formaty eksportowania zdarzenia do systemu SIEM

System SIEM	Format eksportu
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - dostosowany format zdarzeń dla IBM Security QRadar SIEM. QRadar może integrować, identyfikować i przetwarzać zdarzenia LEEF. Zdarzenia LEEF muszą używać kodowania UTF-8. Szczegółowe informacje na temat protokołu LEEF można znaleźć w Centrum wiedzy IBM.

- CEF (Common Event Format)—standard zarządzania dziennikami, który ulepsza współdziałanie zdarzeń dotyczących bezpieczeństwa między różnymi urządzeniami i aplikacjami sieciowymi i zabezpieczającymi. CEF umożliwia korzystanie z podstawowego formatu dziennika zdarzeń, co ułatwia integrowanie i gromadzenie danych do analizy przez system zarządzania korporacji.

Automatyczne eksportowanie oznacza, że Kaspersky Security Center wysyła ogólne zdarzenia do systemu SIEM. Automatyczne eksportowanie zdarzeń rozpoczyna się od razu po włączeniu tej opcji. Ta sekcja szczegółowo wyjaśnia, jak włączyć automatyczne eksportowanie zdarzeń.

Informacje dotyczące eksportowania zdarzeń przy użyciu formatu Syslog

Możesz użyć formatu Syslog do wyeksportowania do systemów SIEM zdarzeń, które występują na Serwerze administracyjnym i w innych aplikacjach firmy Kaspersky, zainstalowanych na zarządzanych urządzeniach.

Protokół Syslog jest standardowym protokołem rejestrowania wiadomości. Pozwala on na rozdzielenie oprogramowania, które generuje wiadomości, systemu, które je przechowuje, oraz oprogramowania, które raportuje i analizuje te wiadomości. Do każdej wiadomości przypisywany jest kod funkcji, wskazujący typ oprogramowania, które generuje wiadomość, oraz priorytet.

Format Syslog jest definiowany przez dokumenty RFC (Request for Comments — prośba o komentarze), publikowane przez Internet Engineering Task Force (standardy internetowe). Standard RFC 5424 jest używany do eksportowania zdarzeń z Kaspersky Security Center do systemów zewnętrznych.

W Kaspersky Security Center możesz skonfigurować eksportowanie zdarzeń do systemów zewnętrznych przy użyciu formatu Syslog.

Proces eksportowania składa się z dwóch etapów:

1. Włączanie automatycznego eksportowania zdarzeń. W tym kroku program Kaspersky Security Center jest konfigurowany tak, aby wysyłał zdarzenia do systemu SIEM. Kaspersky Security Center rozpoczyna wysyłanie

zdarzeń natychmiast po włączeniu automatycznego eksportowania.

2. Wybieranie zdarzeń eksportowanych do systemu zewnętrznego. W tym kroku wybierasz zdarzenia, które będą eksportowane do systemu SIEM.

Konfigurowanie Kaspersky Security Center do wyeksportowania zdarzeń do systemu SIEM

Ten artykuł opisuje sposób skonfigurowania eksportowania zdarzeń do systemów SIEM.

W celu skonfigurowania eksportowania do systemów SIEM w Kaspersky Security Center Web Console:

1. W menu głównym przejdź do sekcji **Ustawienia konsoli** → **Integracja**.
2. Na zakładce **Integracja** wybierz sekcję **SIEM**.
3. Kliknij odnośnik **Ustawienia**.

   Zostanie otwarta sekcja **Eksportuj ustawienia**.
4. W sekcji **Eksportuj ustawienia** określ ustawienia:

   - **Adres serwera systemu SIEM**

     Adres IP serwera, na którym zainstalowany jest aktualnie używany system SIEM. Sprawdź wartość tego ustawienia w ustawieniach systemu SIEM.

   - **Port systemu SIEM**

     Numer portu używanego do nawiązania połączenia pomiędzy Kaspersky Security Center a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center i w ustawieniach odbiornika Twojego systemu SIEM.

   - **Protokół**

Wybierz protokół, który będzie używany do przesyłania wiadomości do systemu SIEM. Możesz wybrać protokół TCP/IP, UDP lub TLS przez protokół TCP.

Określ następujące ustawienia TLS, jeśli wybierzesz TLS poprzez protokół TCP:

- **Uwierzytelnianie serwera**

  W polu **Uwierzytelnianie serwera** możesz wybrać wartości **Zaufane certyfikaty** lub **Odciski palców SHA**:

  - **Zaufane certyfikaty**. Możesz otrzymać plik z listą certyfikatów od zaufanych urzędów certyfikacji (CA) i przesłać go do Kaspersky Security Center. Kaspersky Security Center sprawdza, czy certyfikat serwera systemu SIEM jest również podpisany przez zaufany urząd certyfikacji, czy nie.

    Aby dodać zaufany certyfikat, kliknij przycisk **Przeglądaj w poszukiwaniu pliku certyfikatów urzędu certyfikacji**, a następnie prześlij certyfikat.

  - **Odciski palców SHA**. Możesz określić odciski palców SHA-1 certyfikatów systemu SIEM w Kaspersky Security Center. Aby dodać odcisk palca SHA-1, wprowadź go w polu **Odciski kciuka** palców, a następnie kliknij przycisk **Dodaj**.

  Korzystając z ustawienia **Dodaj uwierzytelnianie klienta**, możesz wygenerować certyfikat do uwierzytelnienia Kaspersky Security Center. W ten sposób będziesz używać certyfikatu z podpisem własnym wystawionego przez Kaspersky Security Center. W takim przypadku do uwierzytelnienia serwera systemu SIEM można użyć zarówno zaufanego certyfikatu, jak i odcisku palca SHA.

- **Dodaj nazwę podmiotu / nazwę alternatywną podmiotu**

  Nazwa podmiotu to nazwa domeny, dla której otrzymano certyfikat. Kaspersky Security Center nie może połączyć się z serwerem systemu SIEM, jeśli nazwa domeny serwera systemu SIEM nie jest zgodna z nazwą podmiotu certyfikatu serwera systemu SIEM. Jednak serwer systemu SIEM może zmienić swoją nazwę domeny, jeśli zmieniła się nazwa w certyfikacie. W takim przypadku można określić nazwy podmiotów w polu **Dodaj nazwę podmiotu / nazwę alternatywną podmiotu**. Jeśli dowolna z podanych nazw podmiotów odpowiada nazwie podmiotu certyfikatu systemu SIEM, Kaspersky Security Center zweryfikuje certyfikat serwera systemu SIEM.

- **Dodaj uwierzytelnianie klienta**

  W celu uwierzytelnienia klienta możesz wstawić swój certyfikat lub wygenerować go w Kaspersky Security Center.

  - **Wstaw certyfikat**. Możesz użyć certyfikatu otrzymanego z dowolnego źródła, na przykład, z dowolnego zaufanego urzędu certyfikacji. Musisz określić certyfikat i jego klucz prywatny, używając jednego z następujących typów certyfikatów:

    - **Certyfikat X.509 PEM**. Prześlij plik z certyfikatem w polu **Plik z certyfikatem** oraz plik z kluczem prywatnym w polu **Plik z kluczem**. Oba pliki nie są od siebie zależne, a kolejność wczytywania plików nie ma znaczenia. Po przesłaniu obu plików określ hasło do dekodowania klucza prywatnego w polu **Weryfikacja hasła lub certyfikatu**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

    - **Certyfikat X.509 PKCS12**. Prześlij pojedynczy plik zawierający certyfikat i jego klucz prywatny w polu **Plik z certyfikatem**. Po przesłaniu pliku określ hasło do dekodowania klucza prywatnego w polu **Weryfikacja hasła lub certyfikatu**. Hasło może mieć pustą wartość, jeśli klucz prywatny nie jest zakodowany.

- **Generuj klucz**. Możesz wygenerować certyfikat z podpisem własnym w Kaspersky Security Center. W rezultacie Kaspersky Security Center przechowuje wygenerowany certyfikat z podpisem własnym i możesz przekazać publiczną część certyfikatu lub odcisk palca SHA1 do systemu SIEM.

- **Format danych**

  Możesz wybrać formaty Syslog, CEF lub LEEF, w zależności od wymagań systemu SIEM.

Jeśli wybierzesz format Syslog, musisz określić:

- **Maksymalny rozmiar wiadomości zdarzenia w bajtach**

  Określ maksymalny rozmiar (w bajtach) jednej wiadomości przekazywanej do systemu SIEM. Każde zdarzenie jest przesyłane w jednej wiadomości. Jeśli rzeczywisty rozmiar wiadomości przekracza określoną wartość, wiadomość jest skracana i dane mogą zostać utracone. Domyślny rozmiar to 2048 bajtów. To pole jest dostępne tylko wtedy, gdy w polu **Protokół** wybrałeś format Syslog.

5. Przełącz opcję na pozycję **Automatycznie eksportuj zdarzenia do bazy danych systemu SIEM Włączone**.
6. Kliknij przycisk **Zapisz**.

Eksportowanie do systemu SIEM zostało skonfigurowane.

Eksportowanie zdarzeń bezpośrednio z bazy danych

Zdarzenia można otrzymywać bezpośrednio z bazy danych Kaspersky Security Center bez konieczności korzystania z interfejsu Kaspersky Security Center. Możesz wykonać zapytanie bezpośrednio do widoków publicznych i pobrać dane zdarzenia lub utworzyć swoje własne widoki w oparciu o istniejące widoki publiczne i adresować je w celu otrzymania żądanych danych.

Widoki publiczne

Dla Twojej wygody, w bazie danych Kaspersky Security Center dostępny jest zestaw widoków publicznych. Opis tych widoków publicznych można znaleźć w dokumentacji klakdb.chm.

Widok publiczny v_akpub_ev_event zawiera zestaw pól, które reprezentują parametry zdarzenia w bazie danych. W dokumencie klakdb.chm możesz także znaleźć informacje dotyczące widoków publicznych odpowiadających innym obiektom Kaspersky Security Center, na przykład: urządzeniom, aplikacjom lub użytkownikom. Możesz użyć tych informacji w swoich zapytaniach.

Ta sekcja zawiera instrukcje dotyczące tworzenia zapytania SQL przy użyciu narzędzia klsql2 oraz przykłady zapytań.

Aby utworzyć zapytania SQL lub widoki bazy danych, możesz także użyć innego dowolnego programu do pracy z bazami danych. Informacje dotyczące przeglądania parametrów połączenia z bazą danych Kaspersky Security Center, takich jak nazwa instancji i nazwa bazy danych, znajdują się w odpowiedniej sekcji.

Tworzenie zapytania SQL przy użyciu narzędzia klsql2

Ta sekcja opisuje sposób pobierania i korzystania z narzędzia klsql2, a także sposób tworzenia zapytań SQL przy użyciu tego narzędzia.

W celu pobrania i użycia narzędzia klsql2:

1. Pobierz narzędzie klsql2 ze strony internetowej Kaspersky. Nie używaj wersji narzędzia klsql2 przeznaczonych dla starszych wersji Kaspersky Security Center.
2. Skopiuj i rozpakuj pobrany plik klsql2.zip do dowolnego folderu na urządzeniu z zainstalowanym Serwerem administracyjnym Kaspersky Security Center.

   Pakiet klsql2.zip zawiera następujące pliki:

   - klsql2.exe
   - src.sql
   - start.cmd
3. Otwórz plik src.sql w dowolnym edytorze tekstu.
4. W pliku src.sql wpisz typ żądanego zapytania SQL, a następnie zapisz plik.
5. Na urządzeniu z zainstalowanym Serwerem administracyjnym Kaspersky Security Center, w wierszu polecenia wpisz następujące polecenie do uruchomienia zapytania SQL z pliku src.sql i zapisz wyniki do pliku result.xml:

   ```
   klsql2 -i src.sql -u <nazwa użytkownika> -p <hasło> -o result.xml
   ```

   gdzie `<nazwa użytkownika>` i `<hasło>` to poświadczenia konta użytkownika, który ma dostęp do bazy danych.
6. W razie potrzeby wprowadź login i hasło konta użytkownika, który ma dostęp do bazy danych.
7. Otwórz nowo utworzony plik result.xml, aby wyświetlić wyniki zapytania SQL.

Możesz zmodyfikować plik src.sql i utworzyć dowolne zapytanie SQL do widoków publicznych. Następnie, z poziomu wiersza poleceń, wykonaj zapytanie SQL i zapisz wyniki do pliku.

Przykład zapytania SQL w narzędziu klsql2

W tej sekcji przedstawiono przykład zapytania SQL, utworzonego przy użyciu narzędzia klsql2.

Poniższy przykład ilustruje otrzymanie zdarzeń, które wystąpiły na urządzeniach w ciągu ostatnich siedmiu dni, oraz wyświetlenie zdarzeń według czasu ich wystąpienia (najnowsze są wyświetlane jako pierwsze).

Na przykład:

```
SELECT
e.nId, /* identyfikator zdarzenia */
e.tmRiseTime, /* godzina wystąpienia zdarzenia */
e.strEventType, /* wewnętrzna nazwa typu zdarzenia */
e.wstrEventTypeDisplayName, /* wyświetlona nazwa zdarzenia */
e.wstrDescription, /* wyświetlony opis zdarzenia */
e.wstrGroupName, /* nazwa grupy, w której znajduje się zdarzenie */
```

```
h.wstrDisplayName, /* wyświetlona nazwa urządzenia, na którym wystąpiło zdarzenie */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* adres IP urządzenia, na którym
wystąpiło zdarzenie */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Sprawdzanie nazwy bazy danych Kaspersky Security Center

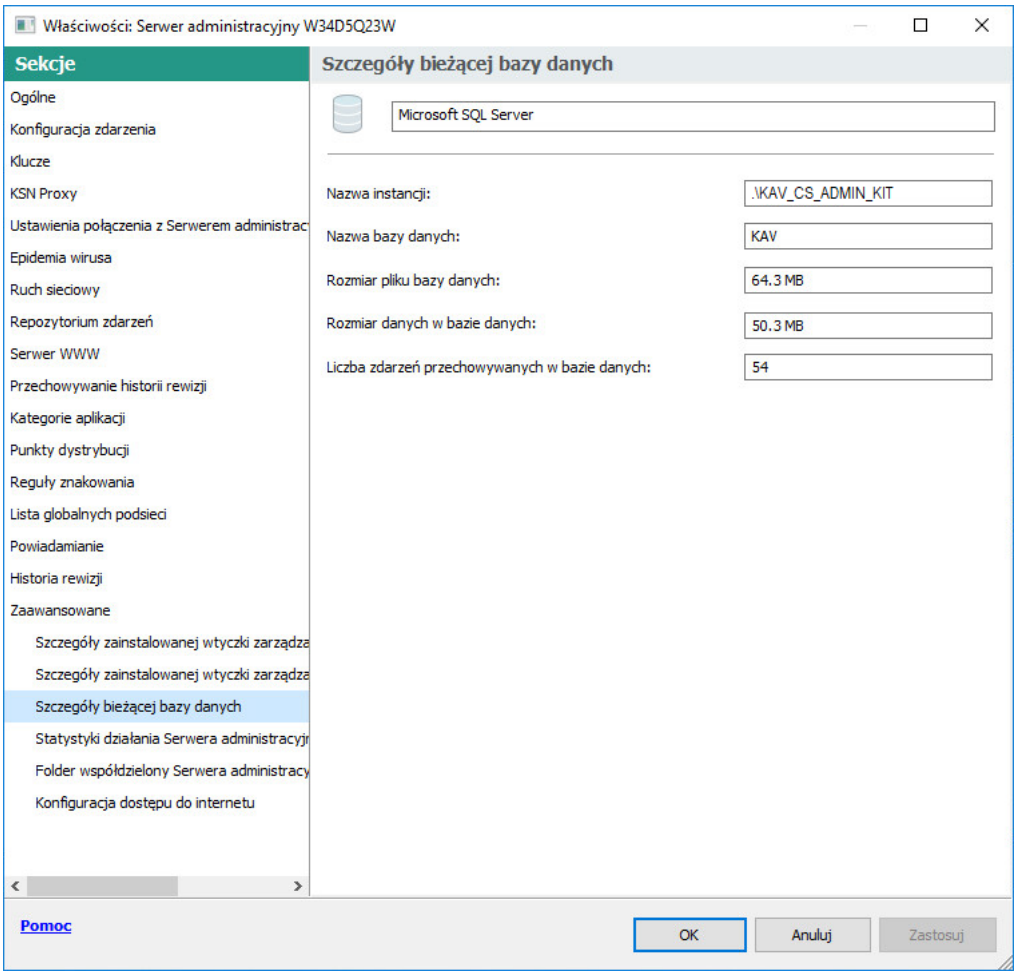
Znajomość nazwy bazy danych może być pomocna, jeśli na przykład trzeba wysłać zapytanie SQL i połączyć się z bazą danych z edytora skryptów SQL.

W celu wyświetlenia nazwy bazy danych Kaspersky Security Center:

1. W drzewie konsoli Kaspersky Security Center otwórz menu kontekstowe folderu **Serwer administracyjny** i wybierz **Właściwości**.
2. W oknie właściwości Serwera administracyjnego, w panelu Sekcje wybierz **Zaawansowane**, a następnie **Szczegóły bieżącej bazy danych**.
3. W sekcji **Szczegóły bieżącej bazy danych** zwróć uwagę na następujące właściwości bazy danych (patrz rysunek poniżej):
   - Nazwa instancji

     Nazwa bieżącej instancji bazy danych Kaspersky Security Center. Domyślna wartość to *.\KAV_CS_ADMIN_KIT*.
   - Nazwa bazy danych

     Nazwa bazy danych SQL Kaspersky Security Center. Domyślna wartość to *KAV*.



Sekcja z informacjami o bieżącej bazie danych Serwera administracyjnego

4. Kliknij przycisk **OK**, aby zamknąć okno właściwości Serwera administracyjnego.

Użyj nazwy bazy danych, aby adresować bazę danych w swoich zapytaniach SQL.

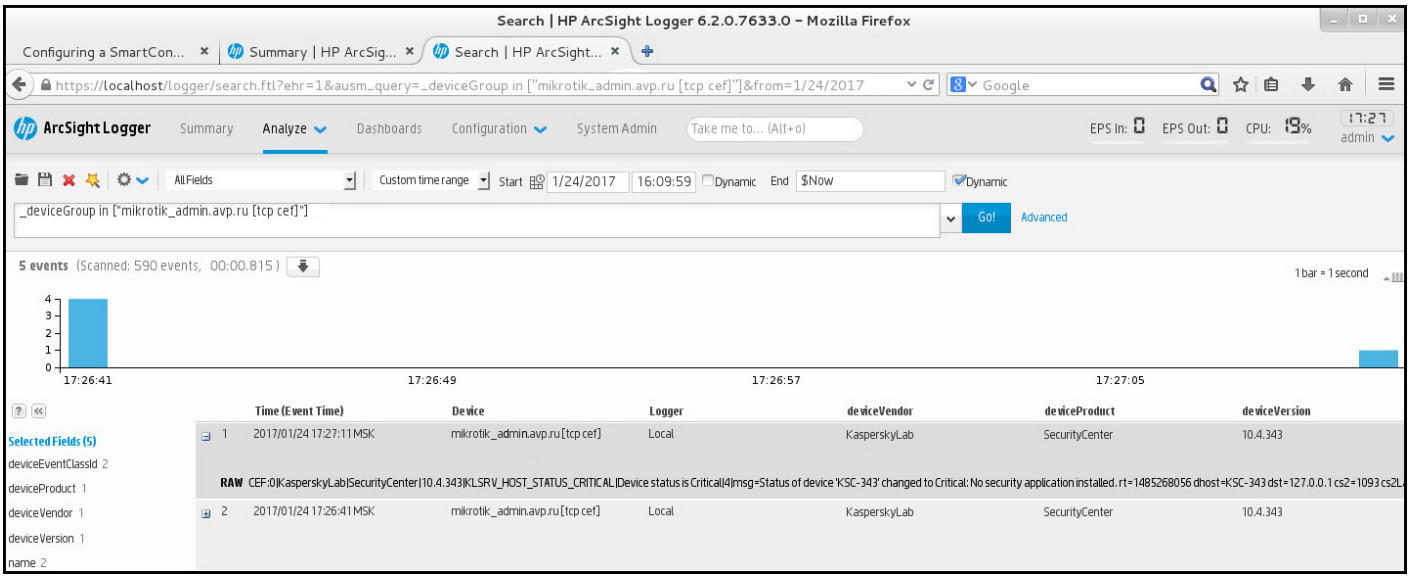
Przeglądanie wyników eksportowania

Możesz kontrolować pomyślne zakończenie procedury eksportowania zdarzeń. W tym celu sprawdź, czy wiadomości z eksportowanymi zdarzeniami są otrzymywane przez Twój system SIEM.

Jeśli zdarzenia wysłane z Kaspersky Security Center są odbierane i poprawnie analizowane przez Twój system SIEM, konfiguracja po obu stronach została przeprowadzona właściwie. Jeśli jest inaczej, sprawdź ustawienia, które określiłeś w Kaspersky Security Center, porównując je z konfiguracją w Twoim systemie SIEM.

Poniższy rysunek przedstawia zdarzenia wyeksportowane do ArcSight. Na przykład, pierwsze zdarzenie jest krytycznym zdarzeniem Serwera administracyjnego: „*Urządzenie posiada stan Krytyczny*”.

Reprezentacja eksportowania zdarzeń w systemie SIEM różni się w zależności od tego, którego systemu SIEM używasz.



Przykład zdarzeń

Praca z Kaspersky Security Center Web Console w środowisku chmury

Ta sekcja zawiera informacje o funkcjach Kaspersky Security Center Web Console dotyczących zdalnej instalacji i konserwacji Kaspersky Security Center w środowiskach chmury, takich jak Amazon Web Services, Microsoft Azure lub Google Cloud.

Aby móc pracować w obrębie środowiska chmury, potrzebna jest specjalna licencja. Jeśli nie posiadasz takiej licencji, elementy interfejsu dotyczące urządzeń w chmurze nie są wyświetlane.

Konfiguracja środowiska chmury w Kaspersky Security Center Web Console

Aby skonfigurować Kaspersky Security Center przy użyciu Kreatora konfiguracji środowiska chmury, musisz mieć:

- Następujące dane uwierzytelniające środowiska w chmurze:
  - Rolę IAM, której udzielono uprawnienie do przeszukiwania segmentu chmury lub konto użytkownika IAM, któremu udzielono uprawnienia do przeszukiwania segmentu chmury (do pracy z Amazon Web Services)
  - ID aplikacji Azure, hasło i subskrypcję (do pracy z Microsoft Azure)
  - Poczta klienta Google, ID projektu i klucz prywatny (do pracy z Google Cloud)
- Pakiety instalacyjne:
  - Agent sieciowy dla systemu Windows
  - Agent sieciowy dla systemu Linux
  - Kaspersky Endpoint Security for Linux
- Wtyczka sieciowa dla Kaspersky Endpoint Security for Linux
- Wybierz jeden z następujących:

- Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Endpoint Security for Windows (zalecane)
- Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Security for Windows Server

Kreator konfiguracji środowiska chmury uruchamia się automatycznie przy pierwszym połączeniu z Serwerem administracyjnym za pośrednictwem Konsoli administracyjnej, jeśli program Kaspersky Security Center jest instalowany za pomocą gotowego do użycia obrazu. Kreator można również uruchomić ręcznie w dowolnym momencie.

Aby ręcznie uruchomić Kreatora konfiguracji środowiska chmury:

W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Konfiguruj środowisko chmury**.

Zostanie uruchomiony kreator.

Przeciętna sesja pracy nad konfiguracją środowiska chmury trwa około 15 minut.

Krok 1. Sprawdzanie wymaganych wtyczek i pakietów instalacyjnych

Ten krok nie jest wyświetlany, jeśli masz wszystkie wymagane wtyczki internetowe i pakiety instalacyjne wymienione poniżej.

Aby skonfigurować środowisko w chmurze, musisz mieć następujące komponenty:

- Pakiety instalacyjne:
  - Agent sieciowy dla systemu Windows
  - Agent sieciowy dla systemu Linux
  - Kaspersky Endpoint Security for Linux
- Wtyczka sieciowa dla Kaspersky Endpoint Security for Linux
- Wybierz jeden z następujących:
  - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Endpoint Security for Windows (zalecane)
  - Pakiet instalacyjny i wtyczka sieciowa dla Kaspersky Security for Windows Server

    Zalecamy używanie Kaspersky Endpoint Security for Windows zamiast Kaspersky Security for Windows Server.

Kaspersky Security Center automatycznie wykrywa komponenty, które już posiadasz i wyświetla listę tylko tych, których brakuje. Pobierz wymienione komponenty, klikając przycisk **Wybierz aplikacje do pobrania**, a następnie wybierając wymagane wtyczki i pakiety instalacyjne. Po pobraniu składnika można użyć przycisku **Odśwież**, aby zaktualizować listę brakujących składników.

Krok 2. Licencjonowanie aplikacji

Ten krok jest wyświetlany tylko wtedy, gdy używasz BYOL AMI i nie aktywowałeś aplikacji przy użyciu licencji dla Kaspersky Security for Virtualization lub licencji dla Kaspersky Hybrid Cloud Security.

Określ klucz licencyjny i kliknij **Dalej**, aby przejść dalej.

Klucz licencyjny, który określiłeś, zostanie dodany do repozytorium Serwera administracyjnego.

Jeśli uruchomisz kreator ponownie, ten krok nie będzie wyświetlany.

Krok 3. Wybieranie środowiska chmury i autoryzacji

Ta sekcja opisuje funkcje stosowane tylko do Kaspersky Security Center 12.1 lub nowszej wersji.

Określ następujące ustawienia:

- **Środowisko chmury**

  Wybierz środowisko chmury, w którym instalujesz Kaspersky Security Center: AWS, Azure lub Google Cloud.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem w chmurze, wybierz jedno środowisko, a następnie uruchom kreator ponownie.

- **Nazwa połączenia**

  Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

  Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

  Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment”, „AWS Segment” lub „Google Segment”.

Wprowadź swoje dane uwierzytelniające do autoryzacji w środowisku chmury.

AWS

Jeśli jako typ segmentu chmury wybrałeś AWS, potrzebujesz roli IAM lub klucza dostępu AWS IAM do dalszego przeszukiwania segmentu chmury.

- **Rola AWS IAM przypisana do instancji EC2**

  Wybierz tę opcję, jeśli posiadasz rolę IAM z wymaganymi uprawnieniami dla Serwera administracyjnego.

- **Użytkownik AWS IAM**

Wybierz tę opcję, jeśli posiadasz klucz dostępu AWS IAM. Wprowadź swoje dane klucza:

- **Identyfikator klucza dostępu**

  Identyfikator klucza dostępu IAM to sekwencja znaków alfanumerycznych. Identyfikator klucza otrzymałeś podczas tworzenia konta użytkownika IAM.

  Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

- **Klucz tajny**

  Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

  Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

  Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

Azure

Jeśli jako typ segmentu chmury wybrałeś Azure, określ następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **ID aplikacji Azure**

  Ten ID aplikacji utworzyłeś na portalu Azure.

  Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **ID subskrypcji platformy Azure**

  Subskrypcję utworzyłeś na portalu Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **Klucz dostępu do magazynu Azure**

Hasło (klucz) uzyskałeś po utworzeniu konta magazynu Azure do pracy z Kaspersky Security Center.

Klucz jest dostępny w sekcji „Overview of the Azure storage account", w podsekcji „Keys".

Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

Google Cloud

Jeśli jako typ segmentu chmury wybrałeś Google Cloud, określ następujące ustawienia dla połączenia, które będą używane do dalszego przeszukiwania segmentu chmury:

- **Adres e-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

To połączenie, które określiłeś, zostanie zapisane w ustawieniach aplikacji.

Kreator konfiguracji środowiska chmury umożliwia określenie tylko jednego segmentu. Później możesz określić więcej połączeń do zarządzania innymi segmentami chmury.

Kliknij **Dalej**, aby przejść dalej.

Krok 4. Przeszukiwanie segmentu, konfigurowanie synchronizacji z chmurą i wybieranie dalszych działań

W tym kroku rozpoczyna się przeszukiwanie segmentu chmury i automatycznie tworzona jest specjalna grupa administracyjna dla urządzeń w chmurze. Urządzenia, wykryte podczas przeszukiwania, zostają umieszczone w tej grupie. Konfigurowany jest terminarz przeszukiwania segmentu chmury (domyślnie, co 5 minut; możesz zmienić to ustawienie później).

Tworzona jest także reguła automatycznego przydzielania **Synchronizuj z chmurą**. Dla każdego kolejnego skanowania sieci chmury, wykryte urządzenia wirtualne zostaną przeniesione do odpowiedniej podgrupy w obrębie grupy **Zarządzane urządzenia\Chmura**.

Określ następujące ustawienia:

- **Synchronizuj grupy administracyjne ze strukturą chmury**

Jeśli ta opcja jest włączona, grupa **Chmura** jest automatycznie tworzona w obrębie grupy **Zarządzane urządzenia** oraz zostaje uruchomione wyszukiwanie urządzeń w chmurze. Instancje i maszyny wirtualne, które zostały wykryte w trakcie każdego skanowania sieci chmury, zostają umieszczone w grupie Chmura. Struktura podgrup administracyjnych w obrębie tej grupy odpowiada strukturze Twojego segmentu chmury (w AWS, strefy dostępności i grupy położenia nie są przedstawione w strukturze; w Azure, podsieci nie są przedstawione w strukturze). Urządzenia, które nie zostały zidentyfikowane jako instancje w środowisku chmury, znajdują się w grupie **Urządzenia nieprzypisane**. Struktura grupa umożliwia korzystanie z grupowych zadań instalacji do zainstalowania aplikacji antywirusowych na instancjach, a także skonfigurowanie różnych zasad dla różnych grup.

Jeśli ta opcja jest wyłączona, tworzona jest także grupa **Chmura** oraz uruchamiane jest wyszukiwanie urządzeń; jednakże podgrupy odpowiadające strukturze segmentu chmury nie są tworzone w obrębie tej grupy. Wszystkie wykryte instancje znajdują się w grupie administracyjnej **Chmura**, więc są wyświetlane na jednej liście. Jeśli Twoja praca z Kaspersky Security Center wymaga synchronizacji, możesz zmodyfikować właściwości reguły **Synchronizuj z chmurą** i wymusić ją. Wymuszenie tej reguły zmieni strukturę podgrup w grupie Chmura tak, że będzie ona odpowiadała strukturze segmentu chmury.

Domyślnie opcja ta jest wyłączona.

- **Roześlij ochronę**

  Jeśli ta opcja jest zaznaczona, kreator tworzy zadanie instalacji aplikacji zabezpieczających na instancjach. Po zakończeniu pracy kreatora, na urządzeniach w Twoich segmentach chmury automatycznie uruchamiany jest Kreator wdrażania ochrony, dzięki czemu możliwe będzie zainstalowanie Agenta sieciowego i aplikacji zabezpieczających na tych urządzeniach.

  Kaspersky Security Center może przeprowadzić zdalną instalację przy użyciu swoich narzędzi. Jeśli nie masz uprawnień do instalowania aplikacji na instancjach EC2 lub maszynach wirtualnych Azure, możesz ręcznie skonfigurować zadanie **Zdalna instalacja** oraz określić konto z wymaganymi uprawnieniami. W tym przypadku, zadanie Zdalna instalacja nie będzie działało dl urządzeń wykrytych przy użyciu AWS API lub Azure. To zadanie będzie działało tylko dla urządzeń wykrytych przy użyciu przeszukiwania Active Directory, przeszukiwania domeny Windows lub przeszukiwania zakresu IP.

  Jeśli ta opcja nie jest zaznaczona, Kreator wdrażania ochrony nie zostanie uruchomiony, a zadania instalacji aplikacji zabezpieczających na instancjach nie zostaną utworzone. Te działania można wykonać ręcznie w późniejszym czasie.

Jeśli wybierzesz opcję Roześlij ochronę, sekcja **Ponowne uruchamianie urządzeń** stanie się dostępna. W tej sekcji musisz wybrać, co zrobić, gdy system operacyjny urządzenia docelowego musi zostać uruchomiony ponownie. Wybierz, czy instancje powinny być uruchamiane ponownie, jeśli system operacyjny urządzenia musi być uruchomiony ponownie podczas instalacji aplikacji:

- **Nie uruchamiaj ponownie**

  Jeśli ta opcja jest zaznaczona, urządzenie nie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

- **Uruchom ponownie**

  Jeśli ta opcja jest zaznaczona, urządzenie zostanie ponownie uruchomione po zainstalowaniu aplikacji zabezpieczającej.

Kliknij **Dalej**, aby przejść dalej.

W przypadku Google Cloud możesz przeprowadzić tylko zdalną instalację natywnych narzędzi Kaspersky Security Center. Jeśli wybrałeś Google Cloud, opcja **Roześlij ochronę** nie jest dostępna.

Krok 5. Wybieranie aplikacji, w odniesieniu do której mają zostać utworzone zasada i zadania

Ten krok jest wyświetlany tylko wtedy, gdy posiadasz pakiety instalacyjne i wtyczki zarówno dla Kaspersky Endpoint Security for Windows, jak i Kaspersky Security for Windows Server. Jeśli masz wtyczkę i pakiet instalacyjny tylko dla jednej z tych aplikacji, ten krok zostanie pominięty, a Kaspersky Security Center utworzy profil i zadania dla istniejącej aplikacji.

Wybierz aplikację, dla której chcesz utworzyć zasadę i zadania:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

Krok 6. Konfigurowanie Kaspersky Security Network dla Kaspersky Security Center

Określ ustawienia przekazywania informacji o działaniach Kaspersky Security Center do bazy wiedzy Kaspersky Security Network (KSN). Wybierz jedną z następujących opcji:

- **Zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje zainstalowane na urządzeniach klienckich automatycznie prześlą szczegóły swoich działań do Kaspersky Security Network. Uczestnictwo w Kaspersky Security Network umożliwia szybsze aktualizowanie baz danych zawierających informacje o wirusach i innych zagrożeniach, co zapewnia szybszą reakcję na pojawiające się zagrożenia bezpieczeństwa.

- **Nie zgadzam się na korzystanie z Kaspersky Security Network**

  Kaspersky Security Center i zarządzane aplikacje nie dostarczą informacji do Kaspersky Security Network.

  Jeśli wybierzesz tę opcję, korzystanie z Kaspersky Security Network zostanie wyłączone.

Kaspersky zaleca uczestniczenie w Kaspersky Security Network.

Mogą zostać wyświetlone także oświadczenia KSN. Jeśli zgodzisz się na korzystanie z Kaspersky Security Network, zarządzana aplikacja będzie wysyłała dane do Kaspersky. Jeśli nie wyrażasz zgody na uczestnictwo w Kaspersky Security Network, zarządzana aplikacja nie wyśle danych do Kaspersky (możesz zmienić to ustawienie w późniejszym czasie w zasadzie aplikacji).

Kliknij **Dalej**, aby przejść dalej.

Krok 7. Tworzenie wstępnej konfiguracji ochrony

Możesz sprawdzić listę utworzonych zasad i zadań.

Zaczekaj, aż tworzenie zasad i zadań zostanie zakończone, a następnie kliknij **Dalej**, aby przejść dalej. Na ostatniej stronie kreatora kliknij przycisk **Zakończ**, aby wyjść.

Przeszukiwanie segmentu sieci za pośrednictwem Kaspersky Security Center Web Console

Informacje o strukturze sieci (i urządzeniach w tej sieci) są otrzymywane przez Serwer administracyjny poprzez regularne przeszukiwanie segmentów chmury przy pomocy narzędzi AWS API, Azure API lub Google API. Kaspersky Security Center używa tych informacji do aktualizacji zawartości folderów: Urządzenia nieprzypisane i Zarządzane urządzenia. Jeżeli skonfigurowałeś automatyczne przenoszenie urządzeń do grup administracyjnych, wykryte urządzenia zostaną włączone do grup administracyjnych.

Aby zezwolić Serwerowi administracyjnemu na przeszukiwanie segmentów chmury, musisz posiadać odpowiednie uprawnienia dla roli IAM lub dla konta użytkownika IAM (w AWS) lub przy pomocy hasła i ID aplikacji (w Azure) lub przy pomocy poczty klienta Google, identyfikatora projektu Google i klucza prywatnego (w Google Cloud).

Możesz dodawać i usuwać połączenia, a także ustawić terminarz przeszukiwania dla każdego segmentu chmury.

Dodawanie połączeń dla przeszukiwania segmentu chmury

W celu dodania połączenia dla przeszukiwania segmentu chmury do listy dostępnych połączeń:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Chmura**.
2. W otwartym oknie kliknij **Właściwości**.
3. W otwartym oknie **Ustawienia** kliknij **Dodaj**.

   Zostanie otwarte okno **Ustawienia segmentu chmury**.
4. Określ nazwę środowiska chmury dla połączenia, która będzie używana do dalszego przeszukiwania segmentu chmury:

   - **Środowisko chmury**

     Wybierz środowisko chmury, w którym instalujesz Kaspersky Security Center: AWS, Azure lub Google Cloud.

     Jeśli planujesz pracować z więcej niż jednym środowiskiem w chmurze, wybierz jedno środowisko, a następnie uruchom kreator ponownie.

   - **Nazwa połączenia**

     Wprowadź nazwę połączenia. Nazwa nie może zawierać więcej niż 256 znaków. Dopuszcza się tylko znaki Unicode.

     Ta nazwa będzie także używana jako nazwa grupy administracyjnej dla urządzeń w chmurze.

     Jeśli planujesz pracować z więcej niż jednym środowiskiem chmury, możesz chcieć uwzględnić nazwę środowiska w nazwie połączenia, na przykład: „Azure Segment”, „AWS Segment” lub „Google Segment”.

5. Wprowadź swoje dane uwierzytelniające do autoryzacji w środowisku chmury.

- Jeśli wybrałeś AWS, określ następujące ustawienia:

  - **Użyj roli AWS IAM**

    Wybierz tę opcję, jeśli już utworzyłeś rolę IAM dla Serwera administracyjnego do korzystania z usług AWS.

  - **Poświadczenia konta użytkownika AWS IAM**

    Wybierz tę opcję, jeśli posiadasz konto użytkownika IAM z wymaganymi uprawnieniami oraz możesz wprowadzić ID klucza oraz tajny klucz.

    Jeśli określiłeś, że posiadasz Poświadczenia konta użytkownika AWS IAM, określ następujące elementy:

    - **Identyfikator klucza dostępu**

      Identyfikator klucza dostępu IAM to sekwencja znaków alfanumerycznych. Identyfikator klucza otrzymałeś podczas tworzenia konta użytkownika IAM.

      Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

    - **Klucz tajny**

      Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

      Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

      Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

    Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

- Jeśli wybrałeś Azure, określ następujące ustawienia:

  - **ID aplikacji Azure**

    Ten ID aplikacji utworzyłeś na portalu Azure.

    Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

  - **ID subskrypcji platformy Azure**

    Subskrypcję utworzyłeś na portalu Azure.

  - **Hasło do aplikacji Azure**

Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

- **Nazwa konta magazynu Azure**

  Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

- **Klucz dostępu do magazynu Azure**

  Hasło (klucz) uzyskałeś po utworzeniu konta magazynu Azure do pracy z Kaspersky Security Center.

  Klucz jest dostępny w sekcji „Overview of the Azure storage account", w podsekcji „Keys".

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

Jeśli wybrałeś Google Cloud, określ następujące ustawienia:

- **Adres e-mail klienta**

  Wprowadź adres e-mail klienta, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Identyfikator projektu**

  Identyfikator projektu to identyfikator, którego użyłeś do zarejestrowania projektu w Google Cloud.

- **Klucz prywatny**

  Klucz prywatny to sekwencja znaków, które otrzymałeś jako klucz prywatny po zarejestrowaniu projektu w Google Cloud. Możesz skopiować i wkleić tę sekwencję, aby uniknąć błędów.

  Aby zobaczyć wprowadzony tajny klucz, kliknij i przytrzymaj przycisk **Pokaż**.

6. Jeśli chcesz, kliknij **Ustaw terminarz przeszukiwania** i zmień ustawienia domyślne.

To połączenie zostanie zapisane w ustawieniach aplikacji.

Po pierwszym przeszukaniu nowego segmentu chmury, w grupie administracyjnej **Zarządzane urządzenia\Chmura** pojawi się podgrupa odpowiadająca temu segmentowi.

Jeśli określisz niepoprawne dane uwierzytelniające, podczas przeszukiwania segmentu chmury nie zostaną wykryte żadne instancje, a nowa podgrupa nie pojawi się w grupie administracyjnej **Zarządzane urządzenia\Chmura**.

Usuwanie połączenia dla przeszukiwania segmentu chmury

Jeśli już nie chcesz przeszukiwać określonego segmentu chmury, możesz usunąć połączenie odpowiadające temu segmentowi z listy dostępnych połączeń. Połączenie można usunąć także wtedy, gdy, na przykład, uprawnienia do przeszukiwania segmentu chmury zostały przeniesione na innego użytkownika, który posiada inne dane uwierzytelniające.

W celu usunięcia połączenia:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie → Wykrywanie → Chmura**.
2. W otwartym oknie kliknij **Właściwości**.
3. W oknie **Ustawienia**, które zostanie otwarte, kliknij nazwę segmentu, który chcesz usunąć.
4. Kliknij **Usuń**.
5. W otwartym oknie kliknij przycisk **OK**, aby potwierdzić swój wybór.

Połączenie zostanie usunięte. Urządzenia w segmencie chmury odpowiadające temu połączeniu są automatycznie usuwane z grup administracyjnych.

Konfigurowanie terminarza przeszukiwania za pośrednictwem Kaspersky Security Center Web Console

Przeszukiwanie segmentu chmury odbywa się zgodnie z terminarzem. Możesz ustawić częstotliwość przeszukiwania.

Częstotliwość przeszukiwania jest automatycznie ustawiana na 5 minut w ustawieniach konfiguracji środowiska chmury. Możesz zmienić tę wartość w dowolnym momencie i ustawić inny terminarz. Nie jest zalecane konfigurowanie wykonywania przeszukiwania z częstotliwością większą niż co 5 minut, ponieważ może to prowadzić do błędów w działaniu AWS API.

W celu skonfigurowania terminarza przeszukiwania segmentu chmury:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie → Wykrywanie → Chmura**.
2. W otwartym oknie kliknij **Właściwości**.
3. W oknie **Ustawienia**, które zostanie otwarte, kliknij nazwę segmentu, dla którego chcesz skonfigurować terminarz przeszukiwania.

   To spowoduje otwarcie okna **Ustawienia segmentu chmury**.
4. W oknie **Ustawienia segmentu chmury** kliknij przycisk **Ustaw terminarz przeszukiwania**.

   Zostanie otwarte okno **Terminarz**.
5. W oknie **Terminarz** określ następujące ustawienia:

   - **Zaplanowane uruchomienie**

     Dostępne są następujące opcje terminarza przeszukiwania:

- **Co N dni**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego dnia i godziny.

  Domyślnie, przeszukiwanie jest uruchamiane codziennie, począwszy od bieżącej daty i godziny systemowej.

- **Co N minut**

  Przeszukiwanie odbywa się regularnie, w określonych przedziałach czasu, począwszy od określonego czasu.

  Domyślnie, przeszukiwanie jest uruchamiane co pięć minut, począwszy od bieżącej czasu systemowego.

- **Według dni tygodnia**

  Przeszukiwanie odbywa się regularnie, w określone dni tygodnia i o określonej godzinie.

  Domyślnie przeszukiwanie jest uruchamiane w każdy piątek o godzinie 18:00:00.

- **Co miesiąc, w określone dni wybranych tygodni**

  Przeszukiwanie odbywa się regularnie, w określone dni miesiąca i o określonej godzinie.

  Domyślnie nie wybrano dni miesiąca; domyślny czas uruchomienia to 18:00:00.

- **Uruchom w przedziale (min)**

  Określ, co oznacza N (minuty lub dni).

- **Począwszy od**

  Określ, kiedy rozpocząć pierwsze przeszukiwanie.

- **Uruchom pominięte zadania**

  Jeśli Serwer administracyjny jest wyłączony lub niedostępny w czasie, dla którego zaplanowane jest przeszukiwanie, Serwer administracyjny może uruchomić przeszukiwanie od razu po jego włączeniu lub odczekać do następnego zaplanowanego przeszukiwania.

  Jeśli ta opcja jest włączona, Serwer administracyjny rozpoczyna przeszukiwanie od razu po jego włączeniu.

  Jeśli ta opcja jest wyłączona, Serwer administracyjny odczekuje do następnego zaplanowanego przeszukiwania.

  Domyślnie opcja ta jest włączona.

6. Kliknij **Zapisz**, aby zachować zmiany.

Terminarz przeszukiwania dla segmentu zostaje skonfigurowany i zapisany.

Przeglądanie wyników przeszukiwania segmentu chmury za pośrednictwem Kaspersky Security Center Web Console

Możesz przejrzeć wyniki przeszukiwania segmentu chmury, przejrzyj listę urządzeń w chmurze, zarządzanych przez Serwer administracyjny.

W celu przejrzenia wyników przeszukiwania segmentu chmury:

W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wykrywanie** → **Chmura**.

Spowoduje to wyświetlenie segmentów chmury dostępnych do przeszukania.

Przeglądanie właściwości urządzeń w chmurze za pośrednictwem Kaspersky Security Center Web Console

Możesz przejrzeć właściwości każdego urządzenia w chmurze.

W celu przejrzenia właściwości urządzenia w chmurze:

1. W menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.
2. Kliknij nazwę urządzenia, którego właściwości chcesz przejrzeć.

   Zostanie otwarte okno właściwości na wybranej sekcji **Ogólne**.
3. Jeśli chcesz przejrzeć właściwości charakterystyczne dla urządzeń w chmurze, w oknie właściwości wybierz sekcję **System**.

   Właściwości są wyświetlane w zależności od platformy w chmurze urządzenia.

   Dla urządzeń w AWS wyświetlane są następujące właściwości:

   - **Urządzenie wykryte przy pomocy API** (wartość: **AWS**)
   - **Region chmury**
   - **Cloud VPC**
   - **Strefa dostępności chmury**
   - **Podsieć chmury**
   - **Grupa położenia w chmurze** (ta jednostka jest wyświetlana tylko wtedy, gdy instancja należy do grupy położenia; w innym przypadku nie jest wyświetlana)

   Dla urządzeń w Azure wyświetlane są następujące właściwości:

   - **Urządzenie wykryte przy pomocy API** (wartość: **Microsoft Azure**)
   - **Region chmury**

- **Podsieć chmury**

Dla urządzeń w Google Cloud wyświetlane są następujące właściwości:

- **Urządzenie wykryte przy pomocy API** (wartość: **Google Cloud**)
- **Region chmury**
- **Cloud VPC**
- **Strefa dostępności chmury**
- **Podsieć chmury**

Synchronizacja z chmurą: konfigurowanie reguły przenoszenia

Podczas operacji Konfiguruj środowisko chmurowe automatycznie tworzona jest reguła Synchronizuj z chmurą. Ta reguła umożliwia automatyczne przenoszenie urządzeń, wykrytych przy każdym przeszukiwaniu, z grupy Urządzenia nieprzypisane do grupy Zarządzane urządzenia\Chmura, aby te urządzenia stały się dostępne dla scentralizowanego zarządzania. Domyślnie, reguła jest aktywna po utworzeniu. Regułę można wyłączyć, zmodyfikować lub wymusić w dowolnym momencie.

W celu zmodyfikowania właściwości reguły Synchronizuj z chmurą i/lub wymuszenia reguły:

1. W menu głównym przejdź do **Wykrywanie i wdrażanie** → **Wdrażanie i przypisywanie** → **Reguły przenoszenia**.

   Spowoduje to otwarcie listy reguł przenoszenia.

2. Na liście reguł przenoszenia wybierz **Synchronizuj z chmurą**.

   Spowoduje to otwarcie okna właściwości reguły.

3. Jeśli to konieczne, określ następujące ustawienia na zakładce **Warunki reguły**, na zakładce **Segmenty chmury**:

   - Urządzenie znajduje się w segmencie chmury

     Reguła jest tylko stosowana do urządzeń, które znajdują się w wybranym segmencie chmury. W innej sytuacji reguła będzie stosowana do wszystkich urządzeń, które zostały wykryte.

     Domyślnie opcja ta jest zaznaczona.

   - Włączając obiekty potomne

     Reguła będzie stosowana do wszystkich urządzeń w wybranym segmencie i we wszystkich zagnieżdżonych podsekcjach chmury. W innym przypadku reguła jest tylko stosowana do urządzeń, które znajdują się w głównym segmencie.

     Domyślnie opcja ta jest zaznaczona.

   - Przenieś urządzenia z obiektów zagnieżdżonych do odpowiednich podgrup

Jeśli ta opcja jest włączona, urządzenia z obiektów zagnieżdżonych zostaną automatycznie przeniesione do podgrup, które odpowiadają ich strukturze.

Jeśli ta opcja jest wyłączona, urządzenia z obiektów zagnieżdżonych zostaną automatycznie przeniesione do głównej podgrupy Chmura bez dalszego rozdzielania.

Domyślnie opcja ta jest włączona.

- Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń

  Jeśli ta opcja jest włączona, gdy struktura grupy **Zarządzane urządzenia\Chmura** nie posiada podgrup, które będą odpowiadały sekcji zawierającej urządzenie, Kaspersky Security Center utworzy takie podgrupy. Na przykład, jeśli nowa podsieć zostanie wykryta podczas wyszukiwania urządzeń, nowa grupa z taką samą nazwą zostanie utworzona w grupie **Zarządzane urządzenia\Chmura**.

  Jeśli ta opcja jest wyłączona, Kaspersky Security Center nie tworzy żadnych nowych podgrup. Na przykład, jeśli nowa podsieć zostanie wykryta podczas przeszukiwania sieci, nowa grupa o tej samej nazwie nie zostanie utworzona w grupie **Zarządzane urządzenia\Chmura**, a urządzenia, które są w tej podsieci, zostaną przeniesione do grupy **Zarządzane urządzenia\Chmura**.

  Domyślnie opcja ta jest włączona.

- Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury

  Jeśli ta opcja jest włączona, aplikacja usunie z grupy Chmura wszystkie podgrupy, które nie odpowiadają żadnym istniejącym obiektom chmury.

  Jeśli ta opcja jest wyłączona, podgrupy, które nie odpowiadają żadnym istniejącym obiektom chmury, zostaną zachowane.

  Domyślnie opcja ta jest włączona.

Jeśli podczas korzystania z kreatora konfiguracji środowiska chmury włączono opcję **Synchronizuj grupy administracyjne ze strukturą chmury**, reguła **Synchronizuj z chmurą** zostanie utworzona z włączonymi opcjami **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń** i **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury**.

Jeśli nie włączyłeś opcji **Synchronizuj grupy administracyjne ze strukturą chmury**, reguła **Synchronizuj z chmurą** zostanie utworzona z wyłączonymi (odznaczonymi) tymi opcjami. Jeśli Twoja praca z Kaspersky Security Center wymaga, aby struktura podgrup w podgrupie **Zarządzane urządzenia \ Chmura** odpowiadała strukturze segmentów chmury, włącz opcje **Utwórz podgrupy odpowiadające kontenerom nowo wykrytych urządzeń** i **Usuń podgrupy, dla których nie odnaleziono odpowiednika w segmentach chmury** we właściwościach reguły, a następnie wymuś regułę.

4. Z listy rozwijalnej **Urządzenie wykryte przy pomocy API** wybierz jedną z następujących wartości:

   - **Nie**. Urządzenie nie może zostać wykryte przy użyciu AWS, Azure lub Google API, co oznacza, że znajduje się poza środowiskiem chmury lub znajduje się w środowisku chmury, ale z jakiegoś powodu nie może zostać wykryte przy użyciu API.
   - **AWS**. Urządzenie jest wykrywane przy pomocy AWS API, co oznacza, że urządzenie znajduje się w środowisku chmury AWS.
   - **Azure**. Urządzenie jest wykrywane przy pomocy Azure API, co oznacza, że urządzenie znajduje się w środowisku chmury Azure.
   - **Google Cloud**. Urządzenie jest wykrywane przy pomocy Google API, co oznacza, że urządzenie znajduje się w środowisku chmury Google.

- Brak wartości. To kryterium nie może zostać zastosowane.

5. Jeśli to konieczne, skonfiguruj inne właściwości reguły w innych sekcjach.

Reguła przenoszenia została skonfigurowana.

Zdalna instalacja aplikacji na maszynach wirtualnych Azure

Aby zainstalować aplikacje na maszynach wirtualnych Microsoft Azure, musisz mieć ważną licencję.

Kaspersky Security Center obsługuje następujące scenariusze:

- Urządzenie klienckie jest wykrywane przy użyciu Azure API; instalacja odbywa się również przy użyciu API. Korzystanie z Azure API oznacza, że możesz zainstalować tylko następujące aplikacje:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- Urządzenie klienckie jest wykrywane za pomocą Azure API; instalacja odbywa się za pośrednictwem punktu dystrybucji lub w przypadku braku punktów dystrybucji ręcznie przy użyciu samodzielnych pakietów instalacyjnych. W ten sposób możesz zainstalować dowolną aplikację obsługiwaną przez Kaspersky Security Center.

Aby utworzyć zadanie zdalnej instalacji aplikacji na maszynach wirtualnych Azure:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. Postępuj zgodnie z instrukcjami kreatora:
   a. Wybierz opcję **Zdalna instalacja aplikacji** jako typ zadania.
   b. Na stronie **Pakiety instalacyjne** wybierz opcję **Zdalna instalacja przez Microsoft Azure API**.
   c. Wybierając konto, aby uzyskać dostęp do urządzeń, użyj istniejącego konta Azure lub kliknij **Dodaj** i wprowadź poświadczenia swojego konta Azure:
      - Nazwa konta Azure

        Wprowadź dowolną nazwę dla określonych poświadczeń. Ta nazwa pojawi się na liście kont do uruchomienia zadania.
      - ID aplikacji Azure

Ten ID aplikacji utworzyłeś na portalu Azure.

Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

- **Hasło do aplikacji Azure**

  Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

  Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

d. Wybierz odpowiednie urządzenia z grupy **Zarządzane urządzenia** \ **Chmura**.

Po zakończeniu pracy kreatora, zadanie zdalnej instalacji aplikacji pojawi się na liście zadań.

Tworzenie zadania Utwórz kopię zapasową danych Serwera administracyjnego przy użyciu systemu DBMS w chmurze

Zadania tworzenia kopii zapasowej są zadaniami Serwera administracyjnego. Tworzysz zadanie tworzenia kopii zapasowej, jeśli chcesz użyć systemu DBMS znajdującego się w środowisku chmury (AWS lub Azure).

W celu utworzenia zadania kopii zapasowej danych Serwera administracyjnego:

1. W menu głównym przejdź do **Urządzenia** → **Zadania**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator tworzenia nowego zadania.
3. W pierwszym kroku kreatora, na liście **Aplikacja** wybierz **Kaspersky Security Center 14.2**, a na liście **Typ zadania** wybierz **Kopia zapasowa danych Serwera administracyjnego**.
4. W odpowiednim kroku kreatora określ następujące informacje:
   - Jeśli pracujesz z bazami danych w AWS:
     - **Nazwa komory S3**

       Nazwa komory S3, którą utworzyłeś dla Kopii zapasowej.

     - **Identyfikator klucza dostępu**

       Identyfikator klucza (sekwencja znaków alfanumerycznych) uzyskałeś podczas tworzenia konta użytkownika IAM do pracy z instancją magazynu komory S3.

       Pole jest dostępne, jeśli w komorze S3 wybrałeś bazę danych RDS.

     - **Tajny klucz**

Tajny klucz, który uzyskałeś z identyfikatorem klucza dostępu podczas tworzenia konta użytkownika IAM.

Znaki klucza tajnego są wyświetlane jako gwiazdki. Jeśli zaczniesz wprowadzać klucz tajny, zostanie wyświetlony przycisk **Pokaż**. Kliknij i przytrzymaj ten przycisk przez wymaganą ilość czasu, aby wyświetlić wprowadzone znaki.

Pole jest dostępne, jeśli do autoryzacji wybrałeś klucz dostępu IAM AWS zamiast roli IAM.

- Jeśli pracujesz z bazami danych w Microsoft Azure:
  - **Nazwa konta magazynu Azure**

    Nazwę konta magazynu Azure utworzyłeś w celu pracy z Kaspersky Security Center.

  - **ID subskrypcji Azure**

    Subskrypcję utworzyłeś na portalu Azure.

  - **Hasło Azure**

    Hasło ID aplikacji uzyskałeś podczas tworzenia ID aplikacji.

    Znaki hasła są wyświetlane jako gwiazdki. Jak tylko zaczniesz wprowadzać hasło, przycisk **Pokaż** stanie się dostępny. Kliknij i przytrzymaj ten przycisk, aby wyświetlić wprowadzane znaki.

  - **ID aplikacji Azure**

    Ten ID aplikacji utworzyłeś na portalu Azure.

    Możesz dostarczyć tylko jeden ID aplikacji Azure dla przeszukiwania i innych celów. Jeśli chcesz przeszukać inny segment Azure, w pierwszej kolejności musisz usunąć istniejące połączenie Azure.

  - **Nazwa serwera Azure SQL**

    Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

  - **Grupa zasobów serwera Azure SQL**

    Nazwa i grupa zasobów są dostępne we właściwościach Twojego serwera Azure SQL.

  - **Klucz dostępu do magazynu Azure**

    Dostępne we właściwościach Twojego konta magazynu, w sekcji Klucze dostępu. Możesz użyć dowolnego klucza (key1 lub key2).

Zadanie zostanie utworzone i będzie wyświetlane na liście zadań. Jeśli włączyłeś opcję **Otwórz szczegóły zadania po jego utworzeniu**, możesz zmodyfikować domyślne ustawienia zadania od razu po utworzeniu zadania. Jeśli nie włączysz tej opcji, zadanie zostanie utworzone z domyślnymi ustawieniami. Możesz zmodyfikować domyślne ustawienia później w dowolnym momencie.

Zdalna diagnostyka urządzeń klienckich

Możesz użyć zdalnej diagnostyki do zdalnego wykonania następujących operacji na urządzeniach klienckich:

- Włączania i wyłączania śledzenia, zmieniania poziomu śledzenia i pobierania pliku śledzenia
- Pobierania informacji o systemie i ustawień aplikacji
- Pobierania dzienników zdarzeń
- Generowania pliku zrzutu dla aplikacji
- Uruchamiania diagnostyki i pobierania jej raportów
- Uruchamianie, zatrzymywanie i ponowne uruchamianie aplikacji

Możesz użyć dzienników zdarzeń i raportów diagnostycznych pobranych z urządzenia klienckiego do samodzielnego rozwiązania problemów. Dodatkowo, jeśli skontaktujesz się z działem pomocy technicznej Kaspersky, specjalista z pomocy technicznej może poprosić o pobranie plików śledzenia, plików zrzutu pamięci, dzienników zdarzeń, a także raportów diagnostycznych z urządzenia klienckiego w celu przeprowadzenia dalszej analizy w Kaspersky.

Zdalna diagnostyka odbywa się przy użyciu Serwera administracyjnego.

Otwieranie okna zdalnej diagnostyki

Aby przeprowadzić zdalną diagnostykę na urządzeniu klienckim, powinieneś otworzyć okno zdalnej diagnostyki.

W celu otwarcia okna zdalnej diagnostyki:

1. W celu wybrania urządzenia, dla którego chcesz otworzyć okno zdalnej diagnostyki, wykonaj jedną z następujących czynności:
   - Jeśli urządzenie należy do grupy administracyjnej, w menu głównym przejdź do **Urządzenia** → **Zarządzane urządzenia**.
   - Jeśli urządzenie należy do grupy Urządzenia nieprzypisane, w menu głównym przejdź do **Wykrywanie i wdrażanie** → **Urządzenia nieprzypisane**.
2. Kliknij nazwę żądanego urządzenia.
3. W otwartym oknie właściwości urządzenia wybierz zakładkę **Zaawansowane**.
4. W otwartym oknie kliknij **Zdalna diagnostyka**.

   Spowoduje to otwarcie okna **Zdalna diagnostyka** urządzenia klienckiego.

Włączanie i wyłączanie śledzenia dla aplikacji

Możesz włączyć i wyłączyć śledzenie aplikacji, w tym śledzenie Xperf.

Włączanie i wyłączanie śledzenia

W celu włączenia lub wyłączenia śledzenia na zdalnym urządzeniu:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie do zdalnej diagnostyki kliknij **Zdalna diagnostyka**.
3. W otwartym oknie **Ostrzeżenia i dzienniki** wybierz sekcję **Aplikacje Kaspersky**.

   Spowoduje to otwarcie listy aplikacji firmy Kaspersky zainstalowanych na urządzeniu.
4. Na liście aplikacji wybierz aplikację, dla której chcesz wyłączyć lub wyłączyć śledzenie.

   Zostanie wyświetlona lista opcji zdalnej diagnostyki.
5. Jeśli chcesz włączyć śledzenie:

   a. W sekcji **Śledzenie** listy kliknij **Włącz śledzenie**.

   b. W otwartym oknie **Modyfikuj poziom śledzenia** zalecane jest zachowanie domyślnych wartości ustawień. Jeśli jest to wymagane, specjalista z pomocy technicznej przeprowadzi Cię przez proces konfiguracji. Dostępne są następujące ustawienia:

   - Poziom śledzenia

     Poziom śledzenia definiuje ilość szczegółów, jaką plik śledzenia zawiera.

   - Śledzenie z rotacją plików

     Aplikacja nadpisuje informacje o śledzeniu, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Określ maksymalną liczbę plików, jaka będzie używana do przechowywania informacji o śledzeniu, a także maksymalny rozmiar każdego pliku. Jeśli zostanie zapisana maksymalna liczba plików śledzenia o maksymalnym rozmiarze, najstarszy plik śledzenia zostanie usunięty, aby mógł zostać zapisany nowy plik śledzenia.

     To ustawienie jest dostępne tylko dla Kaspersky Endpoint Security.

   c. Kliknij **Zapisz**.

   Śledzenie jest włączone dla wybranej aplikacji. W niektórych przypadkach, aby włączyć śledzenie, konieczne jest ponowne uruchomienie aplikacji zabezpieczającej i jej zadania.
6. Jeśli chcesz wyłączyć śledzenie dla wybranej aplikacji kliknij **Wyłącz śledzenie**.

   Śledzenie jest wyłączone dla wybranej aplikacji.

Włączanie śledzenia Xperf

W przypadku Kaspersky Endpoint Security specjalista z pomocy technicznej może poprosić o włączenie śledzenia Xperf dla informacji o działaniu systemu.

W celu włączenia i skonfigurowania śledzenia Xperf:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie do zdalnej diagnostyki kliknij **Zdalna diagnostyka**.
3. W otwartym oknie **Ostrzeżenia i dzienniki** wybierz sekcję **Aplikacje Kaspersky**.

   Spowoduje to otwarcie listy aplikacji firmy Kaspersky zainstalowanych na urządzeniu.
4. Na liście aplikacji wybierz Kaspersky Endpoint Security for Windows.

   Zostanie wyświetlona lista opcji zdalnej diagnostyki dla Kaspersky Endpoint Security for Windows.
5. W sekcji **Śledzenie Xperf** listy kliknij **Włącz śledzenie Xperf**.

   Jeśli śledzenie Xperf jest już włączone, zamiast tego zostanie wyświetlony przycisk **Wyłącz śledzenie Xperf**.
6. W otwartym oknie **Zmień poziom śledzenia Xperf**, w zależności od odpowiedzi od specjalisty z pomocy technicznej, wykonaj jedną z następujących czynności:

   a. Wybierz jeden z następujących poziomów śledzenia:

   - **Niski**

     Plik śledzenia tego typu zawiera minimalną ilość informacji o systemie.

     Domyślnie opcja ta jest zaznaczona.

   - **Głęboki**

     Plik śledzenia tego typu zawiera bardziej szczegółowe informacje niż pliki śledzenia typu *Niski* i specjaliści z pomocy technicznej mogą poprosić o nie, gdy plik śledzenia typu *Niski* nie jest wystarczający do oceny działania. *Głęboki* plik śledzenia zawiera informacje techniczne o systemie, w tym informacje o sprzęcie, systemie operacyjnym, listę uruchomionych i zakończonych procesów i aplikacji, zdarzeń użytych do oceny działania, a także zdarzeń z Narzędzia do oceny wydajności systemu Windows.

   b. Wybierz jeden z następujących typów śledzenia Xperf:

   - **Podstawowy**

     Informacje o śledzeniu są otrzymywane podczas działania aplikacji Kaspersky Endpoint Security.

     Domyślnie opcja ta jest zaznaczona.

   - **Po ponownym uruchomieniu**

     Informacje o śledzeniu są otrzymywane, gdy system operacyjny jest uruchamiany na zarządzanym urządzeniu. Ten typ śledzenia jest efektywny, gdy problem, który wpływa na działanie systemu, pojawi się po włączeniu urządzenia, a przed uruchomieniem Kaspersky Endpoint Security.

   Możesz także zostać poproszony o włączenie opcji **Rozmiar pliku, po którym nastąpi nadpisanie, w MB**, aby zapobiec nadmiernemu zwiększeniu rozmiaru pliku śledzenia. Następnie określ maksymalny rozmiar pliku śledzenia. Jeśli plik osiągnie maksymalny rozmiar, najstarsze informacje śledzenia zostaną nadpisane nowymi informacjami.

   c. Zdefiniuj rozmiar pliku rotacji.

d. Kliknij **Zapisz**.

Śledzenie Xperf jest włączone i skonfigurowane.

W celu wyłączenia śledzenia Xperf:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie do zdalnej diagnostyki kliknij **Zdalna diagnostyka**.
3. W otwartym oknie **Ostrzeżenia i dzienniki** wybierz sekcję **Aplikacje Kaspersky**.
   Spowoduje to otwarcie listy aplikacji firmy Kaspersky zainstalowanych na urządzeniu.
4. Na liście aplikacji wybierz Kaspersky Endpoint Security for Windows.
   Zostaną wyświetlone opcje śledzenia dla Kaspersky Endpoint Security for Windows.
5. W sekcji **Śledzenie Xperf** listy kliknij **Wyłącz śledzenie Xperf**.
   Jeśli śledzenie Xperf jest już wyłączone, zamiast tego zostanie wyświetlony przycisk **Włącz śledzenie Xperf**.

Śledzenie Xperf jest wyłączone.

Pobieranie plików śledzenia aplikacji

W celu pobrania pliku śledzenia aplikacji:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie do zdalnej diagnostyki kliknij **Zdalna diagnostyka**.
3. W otwartym oknie **Ostrzeżenia i dzienniki** wybierz sekcję **Aplikacje Kaspersky**.
   Spowoduje to otwarcie listy aplikacji firmy Kaspersky zainstalowanych na urządzeniu.
   W sekcji **Śledzenie** kliknij przycisk **Pliki śledzenia**.
   To spowoduje otwarcie okna **Dzienniki śledzenia urządzenia**, w którym wyświetlana jest lista plików śledzenia.
4. Z listy plików śledzenia wybierz żądany plik.
5. Wykonaj jedną z poniższych czynności:
   - Pobierz wybrany plik, klikając **Pobierz cały plik**.
   - Pobierz porcję wybranego pliku:
     a. Kliknij **Pobierz część**.
     b. W otwartym oknie określ nazwę i fragment pliku do pobrania, zgodnie ze swoimi potrzebami.
     c. Kliknij **Pobierz.**

Wybrany plik lub jego porcja zostają pobrane do lokalizacji, którą określiłeś.

Usuwanie plików śledzenia

Możesz usunąć pliki śledzenia, które nie są już potrzebne.

W celu usunięcia pliku śledzenia:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W otwartym oknie zdalnej diagnostyki kliknij **Zdalna diagnostyka**.
3. W otwartym oknie **Ostrzeżenia i dzienniki** upewnij się, że wybrano sekcję **Dzienniki systemu operacyjnego**.
4. W sekcji **Pliki śledzenia** kliknij przycisk **Raporty usługi Windows Update** lub przycisk **Raporty zdalnej instalacji** w zależności od plików śledzenia, które chcesz usunąć.

   Spowoduje to otwarcie listy plików śledzenia.
5. Z listy plików śledzenia wybierz plik, który chcesz usunąć.
6. Kliknij przycisk **Usuń**.

Wybrany plik śledzenia zostanie usunięty.

Pobierania ustawień aplikacji

W celu pobrania ustawień aplikacji z urządzenia klienckiego:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W otwartym oknie zdalnej diagnostyki kliknij **Zdalna diagnostyka**.
3. W otwartym oknie **Ostrzeżenia i dzienniki** upewnij się, że w prawej sekcji wybrano **Dzienniki systemu operacyjnego**.
   - W sekcji **Informacje o systemie** kliknij przycisk **Pobierz plik**, aby pobrać informacje systemowe o urządzeniu klienckim.
   - W sekcji **Ustawienia aplikacji** kliknij przycisk **Pobierz plik**, aby pobrać informacje o ustawieniach aplikacji zainstalowanych na urządzeniu.

Informacje są pobierane do lokalizacji, którą określiłeś jako plik.

Pobierania dzienników zdarzeń

W celu pobrania dziennika zdarzeń ze zdalnego urządzenia:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie do zdalnej diagnostyki kliknij **Dzienniki urządzenia**.

3. W oknie **Wszystkie dzienniki urządzenia** wybierz odpowiedni dziennik.

4. Wykonaj jedną z poniższych czynności:

   - Pobierz wybrany plik, klikając **Pobierz cały plik**.
   - Pobierz porcję wybranego dziennika:

     a. Kliknij **Pobierz część**.

     b. W otwartym oknie określ nazwę i fragment pliku do pobrania, zgodnie ze swoimi potrzebami.

     c. Kliknij **Pobierz**.

Wybrany dziennik zdarzeń lub jego porcja zostają pobrane do lokalizacji, którą określiłeś.

Uruchamianie, zatrzymywanie, ponowne uruchamianie aplikacji

Aplikację można uruchomić, zatrzymać lub uruchomić ponownie.

W celu uruchomienia, zatrzymania lub ponownego uruchomienia aplikacji:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie do zdalnej diagnostyki kliknij **Zdalna diagnostyka**.
3. W otwartym oknie **Ostrzeżenia i dzienniki** wybierz sekcję **Aplikacje Kaspersky**.
   Spowoduje to otwarcie listy aplikacji firmy Kaspersky zainstalowanych na urządzeniu.
4. Na liście aplikacji wybierz aplikację, którą chcesz uruchomić, zatrzymać lub uruchomić ponownie.
5. Wybierz akcję, klikając jeden z następujących przycisków:

   - **Zatrzymaj aplikację**
     Ten przycisk jest dostępny tylko wtedy, gdy aplikacja jest aktualnie uruchomiona.
   - **Uruchom aplikację ponownie**
     Ten przycisk jest dostępny tylko wtedy, gdy aplikacja jest aktualnie uruchomiona.
   - **Uruchom aplikację**
     Ten przycisk jest dostępny tylko wtedy, gdy aplikacja nie jest aktualnie uruchomiona.

W zależności od wybranej akcji, wymagana aplikacja zostanie uruchomiona, zatrzymana lub uruchomiona ponownie na urządzeniu klienckim.

Jeśli uruchomisz ponownie Agenta sieciowego, zostanie wyświetlona wiadomość informująca, że bieżące połączenie urządzenia z Serwerem administracyjnym zostanie utracone.

Uruchamianie zdalnej diagnostyki aplikacji i pobieranie wyników

W celu uruchomienia diagnostyki aplikacji na zdalnym urządzeniu i pobrania wyników:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W oknie do zdalnej diagnostyki kliknij **Zdalna diagnostyka**.
3. W otwartym oknie **Ostrzeżenia i dzienniki** wybierz sekcję **Aplikacje Kaspersky**.

   Spowoduje to otwarcie listy aplikacji firmy Kaspersky zainstalowanych na urządzeniu.
4. Na liście aplikacji wybierz aplikację, dla której chcesz uruchomić zdalną diagnostykę.

   Zostanie wyświetlona lista opcji zdalnej diagnostyki.
5. W sekcji **Raport diagnostyczny** listy kliknij przycisk **Uruchom diagnostykę**.

   Spowoduje to uruchomienie procesu zdalnej diagnostyki i wygenerowanie raportu diagnostycznego. Po zakończeniu procesu diagnostyki, przycisk **Pobierz raport diagnostyczny** stanie się dostępny.
6. Pobierz raport, klikając przycisk **Pobierz raport diagnostyczny**.

Raport zostanie pobrany do lokalizacji, którą określiłeś.

Uruchamianie aplikacji na urządzeniu klienckim

Konieczne może być uruchomienie aplikacji na urządzeniu klienckim, jeśli specjalista z pomocy technicznej firmy Kaspersky poprosi o to.

Nie trzeba instalować aplikacji na tym urządzeniu.

W celu uruchomienia aplikacji na urządzeniu klienckim:

1. Otwórz okno do zdalnej diagnostyki urządzenia klienckiego.
2. W otwartym oknie zdalnej diagnostyki kliknij **Zdalna diagnostyka**.
3. W otwartym oknie **Ostrzeżenia i dzienniki** wybierz sekcję **Uruchamianie aplikacji zdalnej**.
4. W oknie **Uruchamianie aplikacji zdalnej**, w sekcji **Pliki aplikacji** wybierz jeden z następujących elementów zgodnie z tym, o co poprosi specjalista z Kaspersky:

   - Wybierz archiwum ZIP z aplikacją, którą chcesz uruchomić na urządzeniu klienckim, klikając przycisk **Przeglądaj**.
   - Jeśli to konieczne, określ aplikację wiersza polecenia i jej argumenty.
5. Postępuj zgodnie z instrukcjami specjalisty.

Pobieranie i usuwanie plików z Kwarantanny i Kopii zapasowej

Ta sekcja zawiera informacje na temat pobierania i usuwania plików z Kwarantanny i Kopii zapasowej w Kaspersky Security Center Web Console.

Pobieranie plików z Kwarantanny i Kopii zapasowej

Pliki można pobierać z kwarantanny lub kopii zapasowej tylko wtedy, gdy spełniony jest jeden z dwóch warunków: albo opcja **Nie odłączaj od Serwera administracyjnego** jest włączona w ustawieniach urządzenia lub używana jest brama połączenia. W przeciwnym razie pobieranie nie będzie możliwe.

W celu zapisania kopii pliku z Kwarantanny lub Kopii zapasowej na dysku twardym:

1. Wykonaj jedną z poniższych czynności:

   - Jeśli chcesz zapisać kopię pliku z Kwarantanny, w menu głównym przejdź do **Operacje → Repozytoria → Kwarantanna**.

   - Jeśli chcesz zapisać kopię pliku z Kopii zapasowej, w menu głównym przejdź do **Operacje → Repozytoria → Kopia zapasowa**.

2. W otwartym oknie wybierz plik, który chcesz pobrać, i kliknij **Pobierz**.

   Rozpocznie się pobieranie. Kopia pliku, który został umieszczony w Kwarantannie na urządzeniu klienckim, jest zapisywana w określonym folderze.

Informacje o usuwaniu obiektów z repozytoriów Kwarantanny, Kopii zapasowej lub Aktywnych zagrożeń

Jeśli aplikacje zabezpieczające firmy Kaspersky zainstalowane na urządzeniach klienckich umieszczają obiekty w repozytoriach Kwarantanny, Kopii zapasowej lub Aktywnych zagrożeniach, wysyłają informacje o obiektach dodanych do sekcji **Kwarantanna**, **Kopia zapasowa** lub **Aktywne zagrożenia** w Kaspersky Security Center. Po otwarciu jednej z tych sekcji, wybierz obiekt z listy i kliknij przycisk **Usuń**, a Kaspersky Security Center wykona jedną z następujących akcji lub obie akcje:

- Usunie wybrany obiekt z listy

- Usunie wybrany obiekt z repozytorium

Akcja do wykonania jest definiowana przez aplikację Kaspersky, która umieściła wybrany obiekt w repozytorium. Aplikacja Kaspersky jest określona w polu **Wpis dodany przez**. Zapoznaj się z dokumentacją aplikacji Kaspersky, aby uzyskać szczegółowe informacje o tym, jaka akcja ma zostać wykonana.

Przewodnik po API

Ten podręcznik informacyjny Kaspersky Security Center OpenAPI ma na celu pomóc w następujących zadaniach:

- Automatyzacja i personalizacja. Możesz zautomatyzować zadania, których możesz nie chcieć obsługiwać ręcznie, przy użyciu Konsoli administracyjnej. Możesz także zaimplementować scenariusze niestandardowe, które nie są jeszcze obsługiwane w Konsoli administracyjnej. Na przykład, jako administrator możesz użyć Kaspersky Security Center OpenAPI do tworzenia i uruchamiania skryptów, które ułatwią tworzenie struktury grup administracyjnych i jej aktualizowanie.

- Niestandardowy rozwój. Na przykład, można opracować dla klientów alternatywną Konsolę administracyjną opartą na konsoli MMC, która zezwala na ograniczony zestaw działań.

W przewodniku informacyjnym interfejsu OpenAPI możesz użyć pola wyszukiwania w prawej części ekranu, aby znaleźć potrzebne informacje.

PRZEWODNIK PO OPENAPI

Próbki skryptów

Przewodnik referencyjny OpenAPI zawiera przykłady skryptów Pythona wymienionych w poniższej tabeli. Przykłady pokazują, w jaki sposób można wywoływać metody OpenAPI i automatycznie wykonywać różne zadania w celu ochrony sieci, na przykład utworzyć hierarchię "podstawowa/dodatkowa" , uruchamiać zadania w Kaspersky Security Center lub przypisywać punkty dystrybucji. Możesz uruchamiać próbki bez zmian lub tworzyć własne skrypty na ich podstawie.

Wywoływanie metody OpenAPI i uruchamianie skryptów:

1. Pobierz archiwum KlAkOAPI.tar.gz. To archiwum zawiera pakiet KlAkOAPI i próbki (możesz je skopiować z archiwum lub z przewodnika referencyjnego OpenAPI).

2. Zainstaluj pakiet KlakOAPI z archiwum KlAkOAPI.tar.gz na urządzeniu, na którym zainstalowany jest Serwer administracyjny.

   Możesz wywoływać metody OpenAPI, uruchamiać przykłady i własne skrypty tylko na urządzeniach, na których zainstalowany jest Serwer administracyjny i pakiet KlAkOAPI.

Dopasowywanie scenariuszy użytkowników i próbek metod Kaspersky Security Center OpenAPI

Próbka	Cel próbki	Scenariusz
Zarejestruj KlAkParams	Możesz wyodrębniać i przetwarzać dane za pomocą struktury danych `KlAkParams`. Przykład pokazuje, jak pracować z tą strukturą danych. Przykładowe dane wyjściowe mogą być prezentowane na różne sposoby. Możesz uzyskać dane, aby wysłać metodę HTTP lub użyć ich w swoim kodzie.	Monitorowanie i raportowanie
Utwórz i usuń hierarchię "główny/podrzędny"	Możesz dodać podrzędny Serwer administracyjny i utworzyć hierarchię „główny/podrzędny”. Alternatywnie, możesz odłączyć podrzędny Serwer administracyjny od hierarchii.	• Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego

		Serwera administracyjnego • Usuwanie hierarchii Serwerów administracyjnych
Utwórz hierarchię grup ze strukturą opartą na jednostce Active Directory	Możesz przeszukać jednostkę Active Directory i utworzyć hierarchię wykrytych grup urządzeń.	Tworzenie grup administracyjnych
Utwórz hierarchię grup ze strukturą opartą na buforowanej jednostce Active Directory	Możesz utworzyć hierarchię zarządzanych grup urządzeń w oparciu o wcześniej przeszukiwaną jednostkę Active Directory. Jeśli po ostatnim przeszukiwaniu w Active Directory pojawią się nowe urządzenia, nie zostaną dodane do grupy, ponieważ nie znajdują się w zapisanych wynikach przeszukiwania.	Tworzenie grup administracyjnych
Pobierz pliki listy sieci przez bramę połączenia do określonego urządzenia	Możesz nawiązać połączenie z Agentem sieciowym na żądanym urządzeniu za pomocą bramy połączenia, a następnie pobrać plik z listą sieci na swoje urządzenie.	Dostosowanie punktów dystrybucji i bram połączenia
Zainstaluj klucz licencyjny przechowywany w głównym repozytorium Serwera administracyjnego na dodatkowych Serwerach administracyjnych	Możesz połączyć się z głównym Serwerem administracyjnym, pobrać z niego wymagany klucz licencyjny i przesłać go do wszystkich pomocniczych Serwerów administracyjnych znajdujących się w hierarchii.	Licencjonowanie zarządzanych aplikacji
Utwórz raport obowiązujących uprawnień użytkownika	Możesz utworzyć różne raporty. Na przykład, korzystając z tego przykładu, można wygenerować raport o obowiązujących uprawnieniach użytkownika. Ten raport opisuje uprawnienia, jakie użytkownik posiada, w zależności od jego grupy i roli. Raport można pobrać w formacie HTML, PDF lub Excel.	Generowanie i przeglądanie raportu
Rozpocznij zadanie dla urządzenia	Możesz nawiązać połączenie z Agentem sieciowym na żądanym urządzeniu za pomocą bramy połączenia, a następnie pobrać żądane zadanie.	Ręczne uruchamianie zadania
Utwórz podsieci IP w oparciu o witrynę i usługi Active Directory	Podsieć IP można utworzyć na podstawie używanej jednostki Active Directory. Przykład uruchamia przeszukiwanie określonego zakresu adresów IP i usuwa wykryte podsieci, aby uniknąć ich konfliktu z nową podsiecią. Dlatego nie uruchamiaj tego przykładu w sieci, w której ważne jest zapisanie podsieci.	Konfigurowanie ochrony sieci

	Po przeszukaniu próbka odwołuje się do Active Directory, sprawdza każde znajdujące się w nim urządzenie i tworzy podsieć IP. W tym celu próbka używa masek i adresów IP wszystkich urządzeń.	
Zarejestruj punkty dystrybucji dla urządzeń w grupie	Zarządzane urządzenia można przypisać jako punkty dystrybucji (wcześniej nazywane agentami aktualizacji).	Aktualizowanie baz danych i aplikacji Kaspersky
Wylicz wszystkie grupy	Na grupach administracyjnych możesz wykonać różne akcje. Przykład pokazuje, jak wykonać następujące czynności: • Uzyskaj identyfikator grupy głównej „Zarządzane urządzenia” • Poruszaj się po hierarchii grupy • Pobierz pełną, rozszerzoną hierarchię grup wraz z ich nazwami i zagnieżdżeniem	Konfigurowanie Serwera administracyjnego
Wylicz zadania, przeszukaj statystyki zadań i uruchom zadanie	Możesz znaleźć następujące informacje: • Historia postępu zadania • Aktualny stan zadania • Liczba zadań z różnymi stanami Możesz także uruchomić zadanie. Domyślnie próbka uruchamia zadanie po wygenerowaniu statystyk.	Monitorowanie wykonywania zadania
Utwórz i uruchom zadanie	Możesz utworzyć zadanie. W przykładzie określ następujące parametry zadania: • Typ • Metoda uruchamiania • Nazwa • Grupa urządzeń, dla której będzie używane zadanie Domyślnie, przykład tworzy zadanie typu „Pokaż wiadomość”. Możesz uruchomić to zadanie dla wszystkich zarządzanych urządzeń Serwera administracyjnego. W razie potrzeby możesz określić własne parametry zadania.	Tworzenie zadania
Wylicz klucze licencyjne	Możesz uzyskać listę wszystkich aktywnych kluczy licencyjnych dla aplikacji Kaspersky zainstalowanych na zarządzanych urządzeniach Serwera administracyjnego. Lista zawiera szczegółowe dane o każdym kluczu licencyjnym, takim jak nazwa, typ lub data wygaśnięcia.	Wyświetlanie informacji o używanych kluczach licencyjnych
Utwórz i znajdź użytkownika wewnętrznego	Możesz utworzyć konto do dalszej pracy.	Wybieranie konta do uruchamiania Serwera administracyjnego

Utwórz kategorię niestandardową	Możesz utworzyć kategorię aplikacji z potrzebnymi parametrami.	Tworzenie kategorii aplikacji z zawartością dodaną ręcznie
Wylicz użytkowników przy użyciu SrvView	Możesz użyć klasy SrvView, aby zażądać szczegółowych informacji z serwera administracyjnego. Na przykład, możesz uzyskać listę użytkowników, korzystając z tego przykładu.	Zarządzanie kontami użytkowników

Aplikacje współpracujące z Kaspersky Security Center poprzez interfejs OpenAPI

Niektóre aplikacje współpracują z Kaspersky Security Center poprzez interfejs OpenAPI. Do takich aplikacji należą na przykład Kaspersky Anti Targeted Attack Platform lub Kaspersky Security for Virtualization. Może to być również niestandardowa aplikacja kliencka utworzona przez Ciebie w oparciu o OpenAPI.

Aplikacje współpracujące z Kaspersky Security Center poprzez interfejs OpenAPI łączą się z serwerem administracyjnym. Jeżeli skonfigurowano listę dozwolonych adresów IP do łączenia się z serwerem administracyjnym, dodaj adresy IP urządzeń, na których zainstalowane są aplikacje korzystające z Kaspersky Security Center OpenAPI. Aby dowiedzieć się, czy aplikacja, z której korzystasz, działa z interfejsem OpenAPI, zapoznaj się z sekcją pomocy dla tej aplikacji.

Praktyczne zastosowanie aplikacji dla dostawców usługi

Niniejsza sekcja zawiera informacje dotyczące konfiguracji i korzystania z Kaspersky Security Center.

Ta sekcja zawiera zalecenia dotyczące instalacji, konfiguracji i korzystania z aplikacji, a także opisuje sposoby rozwiązywania typowych problemów występujących podczas działania aplikacji.

Planowanie instalacji Kaspersky Security Center

Podczas planowania instalacji komponentów Kaspersky Security Center w sieci organizacji należy uwzględnić rozmiar i obszar projektu, a zwłaszcza poniższe czynniki:

- Całkowitą liczbę urządzeń.
- Liczbę klientów MSP

Jeden Serwer administracyjny może obsługiwać maksymalnie 100 000 urządzeń. Jeśli całkowita liczba urządzeń w sieci organizacji przekroczy 100 000, wówczas po stronie dostawcy usługi należy zainstalować kilka Serwerów administracyjnych i połączyć je w hierarchię w celu uproszczenia scentralizowanego zarządzania.

Na jednym Serwerze administracyjnym można utworzyć do 500 serwerów wirtualnych, czyli dla każdej grupy 500 klientów MSP potrzebny jest jeden Serwer administracyjny.

Na etapie planowania instalacji należy rozważyć przydzielenie do Serwera administracyjnego specjalnego certyfikatu X.509. Przydzielenie certyfikatu X.509 do Serwera administracyjnego może być przydatne między innymi do:

- Sprawdzania ruchu SSL poprzez kończenie żądań SSL na serwerze proxy
- Określenia wymaganych wartości w polach certyfikatu
- Zapewnienia wymaganej siły szyfrowania certyfikatu

Umożliwianie uzyskania dostępu do Serwera administracyjnego przez Internet

Aby zezwolić urządzeniom w sieci klienckiej na dostęp do Serwera administracyjnego poprzez Internet, należy udostępnić następujące porty Serwera administracyjnego:

- 13000 TCP— port TLS Serwera administracyjnego do podłączania Agentów sieciowych zainstalowanych w sieci klienckiej
- 8061 TCP— port HTTPS do publikowania pakietów autonomicznych przy użyciu narzędzi Konsoli administracyjnej
- 8060 TCP — port HTTP do publikowania pakietów autonomicznych przy użyciu narzędzi Konsoli administracyjnej
- 13292 TCP— port TLS wymagany tylko tam, gdzie konieczne jest zarządzanie urządzeniami mobilnymi

Jeśli chcesz zapewnić klientom podstawowe opcje zarządzania siecią poprzez Kaspersky Security Center Web Console, należy także otworzyć następujące porty Kaspersky Security Center Web Console:

- 8081 TCP— port HTTPS
- Port 8080 TCP—HTTP

Standardowa konfiguracja Kaspersky Security Center

Jeden lub kilka Serwerów administracyjnych jest instalowanych na serwerach MSP. Liczba Serwerów administracyjnych może zostać wybrana w oparciu o dostępny sprzęt, całkowitą liczbę obsługiwanych klientów MSP lub całkowitą liczbę zarządzanych urządzeń.

Jeden Serwer administracyjny może obsługiwać maksymalnie 100 000 urządzeń. Należy rozważyć możliwość zwiększenia liczby zarządzanych urządzeń w najbliższej przyszłości: wygodniejsze może być podłączenie do jednego Serwera administracyjnego mniejszej liczby urządzeń.

Na jednym Serwerze administracyjnym można utworzyć do 500 serwerów wirtualnych, czyli dla każdej grupy 500 klientów MSP potrzebny jest jeden Serwer administracyjny.

Jeśli jest używanych kilka Serwerów, zalecane jest połączenie ich w hierarchię. Korzystanie z hierarchii Serwerów administracyjnych pozwala uniknąć mieszania zasad i zadań, zarządzać całym zbiorem zarządzanych urządzeń tak, jak by były zarządzane przez jeden Serwer administracyjny, czyli wyszukiwać urządzenia, tworzyć wybory urządzeń oraz generować raporty.

Na każdym serwerze wirtualnym, który odpowiada klientowi MSP, należy wskazać jeden lub kilka punktów dystrybucji. Jeśli klienci MSP i Serwer administracyjny są połączone przez Internet, przydatne może być utworzenie zadania *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla punktów dystrybucji, aby mogły one pobierać uaktualnienia bezpośrednio z serwerów Kaspersky, a nie z Serwera administracyjnego.

Jeśli niektóre urządzenia w sieci klienckiej MSP nie mają bezpośredniego dostępu do Internetu, należy przełączyć punkty dystrybucji do trybu bramy połączenia. W tym przypadku Agenty sieciowe na urządzeniach w sieci klienckiej MSP zostaną połączone, w celu dalszej synchronizacji, z Serwerem administracyjnym, ale poprzez bramę, a nie bezpośrednio.

Ponieważ Serwer administracyjny najprawdopodobniej nie będzie mógł przeszukać sieci klienckiej MSP, zalecane jest przekazanie tej funkcji punktowi dystrybucji.

Serwer administracyjny nie będzie mógł wysyłać powiadomień poprzez port UDP o numerze 15000 na zarządzane urządzenia znajdujące się poza NAT w sieci klienckiej MSP. Aby rozwiązać ten problem, we właściwościach urządzeń pełniących rolę punktów dystrybucji i działających w trybie bramy połączenia należy włączyć tryb stałego połączenia z Serwerem administracyjnym (pole **Nie odłączaj od Serwera administracyjnego**). Tryb stałego połączenia jest dostępny, jeśli całkowita liczba punktów dystrybucji nie przekracza 300.

Informacje o punktach dystrybucji

Urządzenie z zainstalowanym Agentem sieciowym mogą być używane jako punkt dystrybucji. W tym trybie Agent sieciowy może wykonywać następujące funkcje:

- Rozsyłać uaktualnienia (mogą być one pobierane z Serwera administracyjnego lub z serwerów Kaspersky). W drugim przypadku należy utworzyć zadanie *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* dla urządzenia pełniącego rolę punktu dystrybucji.

- Instalować oprogramowanie (włączając w to wstępną instalację Agentów sieciowych) na pozostałych urządzeniach.
- Przeszukiwać sieć w celu odnalezienia nowych urządzeń i zaktualizowania informacji o tych istniejących. Punkt dystrybucji może stosować te same metody wykrywania urządzeń co Serwer administracyjny.

Instalacja punktów dystrybucji w sieci organizacji realizuje następujące cele:

- Zmniejsza obciążenie na Serwerze administracyjnym, jeśli działa jako źródło uaktualnień.
- Optymalizuje ruch internetowy, ponieważ, w tym przypadku, każde urządzenie w sieci klienckiej MSP nie musi uzyskać dostępu do serwerów Kaspersky lub Serwera administracyjnego w celu pobrania uaktualnień.
- Zapewnia Serwerowi administracyjnemu dostęp do urządzeń poza NAT (względem Serwera administracyjnego) sieci klienckiej MSP, co umożliwia Serwerowi administracyjnemu wykonanie następujących działań:
  - Wysyłanie powiadomień do urządzeń przez UDP w sieci IPv4 lub IPv6
  - Przeszukiwanie sieci IPv4 lub IPv6
  - Przeprowadzanie wstępnej konfiguracji
  - Pełnienie funkcji serwera push

Punkt dystrybucji jest przydzielony do grupy administracyjnej. W tym przypadku zakres działania punktu dystrybucji obejmuje wszystkie urządzenia w grupie administracyjnej i jej podgrupach. Jednakże urządzenie pełniące funkcję punktu dystrybucji nie musi znajdować się w grupie administracyjnej, do której zostało przydzielone.

Możesz sprawić, że punkt dystrybucji będzie działał jako brama połączenia. W tym przypadku urządzenia objęte zakresem działania tego punktu dystrybucji będą łączyły się z Serwerem administracyjnym poprzez bramę, a nie bezpośrednio. Możesz użyć tego trybu w scenariuszach, które nie zezwalają na nawiązywanie bezpośredniego połączenia między urządzeniami a Agentem sieciowym i Serwerem administracyjnym.

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

Hierarchia Serwerów administracyjnych

W MSP może działać kilka Serwerów administracyjnych. Niewygodne może być zarządzanie kilkoma oddzielnymi Serwerami administracyjnymi, dlatego dobrym wyjściem jest utworzenie hierarchii. Zastosowanie konfiguracji „główny/podrzędny” dla dwóch Serwerów administracyjnych oferuje następujące możliwości:

- Podrzędny Serwer administracyjny dziedziczy profile i zadania od głównego Serwera administracyjnego, zapobiegając dzięki temu powielaniu ustawień.
- Wybory urządzeń na głównym Serwerze administracyjnym mogą zawierać urządzenia z podrzędnych Serwerów administracyjnych.
- Raporty na głównym Serwerze administracyjnym mogą zawierać dane (w tym szczegółowe informacje) z podrzędnych Serwerów administracyjnych.

Wirtualne Serwery administracyjne

W oparciu o fizyczny Serwer administracyjny można utworzyć kilka wirtualnych Serwerów administracyjnych, które będą podobne do podrzędnych Serwerów administracyjnych. W przeciwieństwie do trybu poufnego dostępu, który jest oparty na listach kontroli dostępu (ACL), tryb wirtualnego Serwera administracyjnego jest bardziej funkcjonalny i zapewnia większy stopień izolacji. Jako dodatek do dedykowanej struktury grup administracyjnych dla przypisanych urządzeń z zasadami i zadaniami, każdy wirtualny Serwer administracyjny zawiera swoją grupę nieprzypisanych urządzeń, własne zestawy raportów, wybranych urządzeń i zdarzeń, pakietów instalacyjnych, reguł przenoszenia itd. Dla maksymalnej wspólnej izolacji klientów MSP zalecane jest wybranie wirtualnych Serwerów administracyjnych jako funkcjonalności, która ma zostać użyta. Dodatkowo, utworzenie wirtualnego Serwera administracyjnego dla każdego klienta MSP umożliwia zapewnienie klientom podstawowych opcji zarządzania siecią za pośrednictwem Kaspersky Security Center Web Console.

Wirtualne Serwery administracyjne są bardzo podobne do podrzędnych Serwerów administracyjnych, jednakże posiadają pewne różnice:

- Wirtualny Serwer administracyjny nie posiada większości ustawień globalnych i swoich własnych portów TCP.
- Wirtualny Serwer administracyjny nie posiada podrzędnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny nie posiada innych wirtualnych Serwerów administracyjnych.
- Fizyczny Serwer administracyjny wyświetla urządzenia, grupy, zdarzenia i obiekty na zarządzanych urządzeniach (elementy w Kwarantannie, rejestrze aplikacji itd.) ze wszystkich swoich wirtualnych Serwerów administracyjnych.
- Wirtualny Serwer administracyjny może skanować sieć wyłącznie przy podłączonych punktach dystrybucji.

Zarządzanie urządzeniami mobilnymi z zainstalowanym programem Kaspersky Endpoint Security for Android

Urządzenia mobilne z zainstalowanym programem Kaspersky Endpoint Security for Android™ (zwane dalej "urządzenia KES") są zarządzane przy użyciu Serwera administracyjnego. Kaspersky Security Center obsługuje następujące funkcje zarządzania urządzeniami KES:

- Zarządzanie urządzeniami mobilnymi jak urządzeniami klienckimi:
  - Członkostwo w grupach administracyjnych
  - Monitorowanie, takie jak przeglądanie stanów, zdarzeń i raportów
  - Modyfikowanie ustawień lokalnych i przydzielanie zasad dla Kaspersky Endpoint Security for Android
- Wysyłanie poleceń w sposób scentralizowany
- Zdalne instalowanie pakietów aplikacji mobilnych

Serwer administracyjny zarządza urządzeniami KES przez TLS, port TCP 13292.

Instalacja i wstępna konfiguracja

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

- Serwer administracyjny—główny komponent, zaprojektowany do zarządzania urządzeniami w organizacji i przechowywania danych w DBMS.
- Konsola administracyjna—podstawowe narzędzie administratora. Konsola administracyjna jest dostarczana wraz z Serwerem administracyjnym, ale można ją także zainstalować oddzielnie na jednym lub kilku urządzeniach administratora.
- Kaspersky Security Center Web Console to interfejs sieciowy Serwera administracyjnego, zaprojektowany do wykonywania podstawowych działań. Możesz zainstalować ten komponent na dowolnym urządzeniu, które spełnia wymagania sprzętowe i programowe.
- Agent sieciowy — zaprojektowany do zarządzania aplikacją zabezpieczającą, zainstalowaną na urządzeniu, a także do zbierania informacji o tym urządzeniu. Agenty sieciowe są instalowane na urządzeniach w organizacji.

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

- Instalacja Serwera administracyjnego
- Instalowanie Kaspersky Security Center Web Console
- Instalacja Konsoli administracyjnej na urządzeniu administratora
- Instalacja Agenta sieciowego i aplikacji zabezpieczającej na urządzeniach w firmie

Zalecenia dotyczące instalacji Serwera administracyjnego

Ta sekcja zawiera zalecenia dotyczące instalacji Serwera administracyjnego. Opisane są tu także scenariusze korzystania z folderu współdzielonego na urządzeniu z Serwerem administracyjnym w celu zainstalowania Agenta sieciowego na urządzeniach klienckich.

Tworzenie kont dla usług Serwera administracyjnego na klastrze typu failover

Domyślnie instalator automatycznie tworzy konta bez uprawnień dla usług Serwera administracyjnego. To zachowanie jest najwygodniejsze w przypadku instalacji Serwera administracyjnego na zwykłym urządzeniu.

Jednakże instalacja Serwera administracyjnego na klastrze typu failover wymaga innego scenariusza:

1. Dla usług Serwera administracyjnego utwórz konta domenowe bez uprawnień i przydziel je do globalnej grupy zabezpieczeń w domenie o nazwie KLAdmins.
2. W instalatorze Serwera administracyjnego określ konta domenowe, które zostały utworzone dla usług.

Wybieranie systemu zarządzania bazą danych

Podczas wybierania systemu zarządzania bazą danych (DBMS), który zostanie użyty przez Serwer administracyjny, należy brać pod uwagę liczbę urządzeń podlegających Serwerowi administracyjnemu.

Poniższa tabela zawiera listę prawidłowych opcji DBMS, a także zalecenia i ograniczenia dotyczące ich używania.

DBMS	Zalecenia i ograniczenia
SQL Server Express Edition 2012 lub nowszy	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 10 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń. Jednoczesne korzystanie z systemu DBMS serwera SQL Server Express Edition przez Serwer administracyjny i inną aplikację jest surowo zabronione.
Lokalny serwer SQL Server inny niż Express, 2012 lub nowszy	Brak ograniczeń.
Zdalny serwer SQL Server inny niż Express, 2012 lub nowszy	Ważne tylko wtedy, gdy oba urządzenia są w tej samej domenie Windows®; jeśli domeny są inne, należy nawiązać między nimi obustronną relację zaufania.
Lokalny lub zdalny MySQL 5.5, 5.6 lub 5.7 (MySQL w wersjach 5.5.1, 5.5.2, 5.5.3, 5.5.4 i 5.5.5 nie jest już obsługiwany)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 10 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń.
Lokalny lub zdalny MySQL 8.0.20 lub nowszy	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 50 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń.
Lokalny lub zdalny MariaDB (zobacz obsługiwane wersje)	Użyj tego DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 20 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń.
PostgreSQL, Postgres Pro (zobacz obsługiwane wersje)	Użyj jednego z tych DBMS, jeśli zamierzasz uruchomić pojedynczy Serwer administracyjny do mniej niż 50 000 urządzeń i jeśli nie zamierzasz używać komponentu Kontroli aplikacji do zarządzanych urządzeń.

Jeśli używasz SQL Server 2019 jako DBMS, a nie masz łaty zbiorczej CU12 lub nowszej, po zainstalowaniem Kaspersky Security Center powinieneś wykonać następujące czynności:

1. Nawiąż połączenie z SQL Server przy użyciu SQL Management Studio.
2. Uruchom następujące polecenia (jeśli wybrałeś inną nazwę dla bazy danych, użyj nazwy zamiast KAV):

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. Uruchom ponownie usługę SQL Server 2019.

W przeciwnym razie, korzystanie z SQL Server 2019 może zakończyć się błędem, takim jak „There is insufficient system memory in resource pool 'internal' to run this query".

Określanie adresu Serwera administracyjnego

Podczas instalacji Serwera administracyjnego należy określić zewnętrzny adres Serwera administracyjnego. Podczas tworzenia pakietów instalacyjnych Agenta sieciowego ten adres będzie używany jako domyślny. Wówczas możliwa będzie zmiana adresu komputera z Serwerem administracyjnym przy użyciu narzędzi Konsoli administracyjnej; adres nie zostanie zmieniony automatycznie w już utworzonych pakietach instalacyjnych Agenta sieciowego.

Konfigurowanie ochrony w sieci organizacji klienta

Po zakończeniu instalacji Serwera administracyjnego, zostaje uruchomiona Konsola administracyjna, która oferuje przeprowadzenie wstępnej konfiguracji przy użyciu odpowiedniego kreatora. Jeśli Kreator wstępnej konfiguracji jest uruchomiony, w głównej grupie administracyjnej tworzone są następujące profile i zadania:

- Profil Kaspersky Endpoint Security
- Grupowe zadanie aktualizacji Kaspersky Endpoint Security
- Grupowe zadanie skanowania urządzenia z zainstalowanym programem Kaspersky Endpoint Security
- Profil Agenta sieciowego
- Zadanie wykrywania luk (zadanie Agenta sieciowego)
- Zadanie instalacji uaktualnień i naprawy luk (zadanie Agenta sieciowego)

Profile i zadania są tworzone z domyślnymi ustawieniami, które mogą okazać się nieoptymalne lub nawet niedopuszczalne dla organizacji. Dlatego też należy sprawdzić właściwości utworzonych obiektów i zmodyfikować je ręcznie (jeśli zajdzie taka konieczność).

Ta sekcja zawiera informacje dotyczące ręcznej konfiguracji profili, zadań i innych ustawień Serwera administracyjnego, a także informacje o punkcie dystrybucji, tworzeniu struktury grup administracyjnych i hierarchii zadań oraz innych ustawień.

Ręczna konfiguracja profilu Kaspersky Endpoint Security

W tej sekcji można znaleźć zalecenia dotyczące konfiguracji zasady Kaspersky Endpoint Security, który jest tworzony przez Kreator wstępnej konfiguracji. Możesz przeprowadzić konfigurację w oknie właściwości zasady.

Podczas modyfikowania ustawień należy pamiętać o kliknięciu ikony blokady nad odpowiednim ustawieniem, aby umożliwić jego użycie na stacji roboczej.

Konfigurowanie zasady w sekcji Zaawansowana ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Zaawansowana ochrona przed zagrożeniami** możesz skonfigurować używanie Kaspersky Security Network dla Kaspersky Endpoint Security for Windows. Możesz także skonfigurować moduły Kaspersky Endpoint Security for Windows, takie jak Wykrywanie zachowań, Ochrona przed exploitami, Ochrona przed włamaniami oraz Silnik korygujący.

W podsekcji **Kaspersky Security Network** zalecane jest włączenie opcji **Użyj KSN Proxy**. Użyj tej opcji do redystrybucji i optymalizacji ruchu w sieci. Jeśli opcja **Użyj serwera proxy KSN** jest wyłączona, możesz włączyć bezpośrednie korzystanie z serwerów KSN.

Konfigurowanie profilu w sekcji Podstawowa ochrona przed zagrożeniami

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Ochrona przed podstawowymi zagrożeniami** okna właściwości zasad, zalecamy określenie dodatkowych ustawień w podsekcjach **Zapora sieciowa** i **Ochrona plików**.

Podsekcja **Zapora sieciowa** zawiera ustawienia, które pozwalają kontrolować aktywność sieciową aplikacji na urządzeniach klienckich. Urządzenie klienckie korzysta z sieci, do której przypisany jest jeden z następujących statusów: publiczny, lokalny lub zaufany. W zależności od stanu sieci, Kaspersky Endpoint Security może zezwolić na aktywność sieciową na urządzeniu lub jej zabronić. Gdy dodajesz nową sieć do swojej organizacji, musisz przypisać jej odpowiedni status sieci. Na przykład, jeśli urządzeniem klienckim jest laptop, zalecamy, aby to urządzenie korzystało z sieci publicznej lub zaufanej, ponieważ laptop nie zawsze jest podłączony do sieci lokalnej. W podsekcji **Zapora ogniowa** możesz sprawdzić, czy prawidłowo przypisano stany do sieci używanych w Twojej organizacji.

W celu sprawdzenia listy sieci:

1. We właściwościach zasady przejdź do **Podstawowa ochrona przed zagrożeniami → Zapora sieciowa.**
2. W sekcji **Dostępne sieci** kliknij przycisk **Ustawienia**.
3. W **oknie**, które zostanie otwarte, przejdź do zakładki **Sieci**, aby wyświetlić listę sieci.

W podsekcji **Ochrona plików** możesz wyłączyć skanowanie dysków sieciowych. Skanowanie dysków sieciowych może spowodować znaczne obciążenie dysków sieciowych. Praktyczniejsze jest wykonywanie bezpośredniego skanowania na serwerach plików.

W celu wyłączenia skanowania dysków sieciowych:

1. We właściwościach zasady przejdź do **Podstawowej ochrony przed zagrożeniami → Ochrona plików przed zagrożeniami**.
2. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
3. W otwartym oknie **Ochrona plików**, na zakładce **Ogólne** odznacz pole **Wszystkie dyski sieciowe**.

Konfigurowanie profilu w sekcji Ustawienia ogólne

Pełny opis ustawień w tej sekcji można znaleźć w dokumentacji do Kaspersky Endpoint Security for Windows.

W sekcji **Ustawienia ogólne** okna właściwości profilu zalecamy określenie dodatkowych ustawień w podsekcjach **Raporty i Przechowywanie** oraz **Interfejs**.

W podsekcji **Raporty i przechowywanie** przejdź do sekcji **Przesyłanie danych na Serwer administracyjny**. Pole **informacji o uruchomionej aplikacji** określa, czy baza danych Serwera administracyjnego zapisuje informacje o wszystkich wersjach wszystkich modułów oprogramowania na urządzeniach sieciowych. Jeśli to pole jest zaznaczone, zapisane informacje mogą wymagać znaczącej ilości miejsca na dysku dla bazy danych Kaspersky Security Center (kilkadziesiąt gigabajtów). Odznacz pole **Informacje o uruchomionych aplikacjach**, jeśli wciąż jest zaznaczone w profilu najwyższego poziomu.

Jeśli Konsola administracyjna zarządza ochroną antywirusową w sieci organizacji w trybie scentralizowanym, wyłącz wyświetlanie interfejsu użytkownika Kaspersky Endpoint Security for Windows na stacjach roboczych. W tym celu w podsekcji **Interfejs** przejdź do sekcji **Interakcja z użytkownikiem**, a następnie wybierz opcję **Nie wyświetlaj**.

Aby włączyć ochronę hasłem na stacjach roboczych, w podsekcji **Interfejs** przejdź do sekcji **Ochrona hasłem**, kliknij przycisk **Ustawienia**, a następnie zaznacz pole **Włącz ochronę hasłem**.

Konfigurowanie profilu w sekcji Konfiguracja zdarzenia

W sekcji **Konfiguracja zdarzenia** należy wyłączyć zapisywanie wszelkich zdarzeń na Serwerze administracyjnym, za wyjątkiem następujących zdarzeń:

- Na zakładce **Zdarzenie krytyczne**:
  - Automatyczne uruchamianie aplikacji jest wyłączone
  - Dostęp zabroniony
  - Zablokowano uruchomienie aplikacji
  - Leczenie nie jest możliwe
  - Umowa licencyjna naruszona
  - Nie można załadować modułu szyfrującego
  - Nie można uruchomić dwóch zadań jednocześnie
  - Wykryto aktywne zagrożenie Uruchom Zaawansowane leczenie
  - Wykryto atak sieciowy
  - Nie wszystkie komponenty zostały zaktualizowane
  - Błąd aktywacji
  - Błąd włączenia trybu przenośnego
  - Błąd interakcji z Kaspersky Security Center
  - Błąd wyłączenia trybu przenośnego
  - Błąd zmiany komponentów aplikacji
  - Błąd zastosowania reguł szyfrowania/deszyfrowania pliku
  - Nie można zastosować profilu

- Proces został przerwany
- Zablokowano aktywność sieciową

- Na karcie **Błąd funkcjonalny**: Nieprawidłowe ustawienia zadania. Ustawienia nie zostały zastosowane
- Na zakładce **Ostrzeżenie**:
  - Autoochrona jest wyłączona
  - Nieprawidłowy klucz zapasowy
  - Użytkownik zrezygnował z profilu szyfrowania
- Na karcie **Informacje**: Uruchamianie aplikacji zabronione w trybie testowym

Ręczna konfiguracja grupowego zadania aktualizacji dla Kaspersky Endpoint Security

Informacje zawarte w tej podsekcji odnoszą się tylko do Kaspersky Security Center 10 Maintenance Release 1 i nowszych wersji programu.

Jeśli Serwer administracyjny pełni rolę źródła uaktualnień, optymalna i zalecana opcja terminarza dla Kaspersky Endpoint Security 10 i nowszych wersji to **Po pobraniu nowych uaktualnień do repozytorium** z zaznaczonym polem **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Dla grupowego zadania aktualizacji w Kaspersky Endpoint Security w wersji 8 należy wyraźnie określić opóźnienie uruchamiania (1 godzina lub dłużej) oraz zaznaczyć pole **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Jeśli lokalne zadanie pobierania uaktualnień z serwerów Kaspersky do repozytorium jest tworzone na każdym punkcie dystrybucji, okresowe planowanie będzie optymalne i zalecane dla grupowego zadania aktualizacji Kaspersky Endpoint Security. W tym przypadku, dla przedziału randomizacji należy wybrać wartość - 1 godzina.

Ręczna konfiguracja grupowego zadania skanowania urządzeń z zainstalowanym programem Kaspersky Endpoint Security

Kreator wstępnej konfiguracji tworzy grupowe zadanie skanowania urządzeń. Domyślnie skonfigurowano terminarz **uruchamiania zadania w piątki o godzinie 19:00** z automatyczną randomizacją i odznaczonym polem **Uruchom pominięte zadania**.

Oznacza to, że jeśli urządzenia w organizacji są wyłączone w piątki, na przykład o godzinie 18:30, zadanie skanowania urządzeń nigdy nie zostanie uruchomione. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Konfigurowanie terminarza zadania Wyszukiwanie luk i wymaganych aktualizacji

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego zadanie *Wyszukiwanie luk i wymaganych aktualizacji*. Domyślnie skonfigurowano terminarz **uruchamiania zadania we wtorki o godzinie 19:00** z automatyczną randomizacją i zaznaczonym polem **Uruchom pominięte zadania**.

Jeśli zasady obowiązujące w organizacji nakazują wyłączenie wszystkich urządzeń w tym czasie, zadanie *Wyszukiwanie luk i wymaganych aktualizacji* zostanie uruchomione, gdy urządzenia znowu zostaną włączone, czyli w środę rano. Takie działanie nie jest wskazane, ponieważ wykrywanie luk może zwiększać zużycie procesora i obciążenie podsystemów dysku. Terminarz dla tego zadania należy skonfigurować w oparciu o zasady obowiązujące w organizacji.

Ręczna konfiguracja grupowego zadania instalacji uaktualnień i naprawy luk

Kreator wstępnej konfiguracji tworzy dla Agenta sieciowego grupowe zadanie instalacji uaktualnień i naprawy luk. Domyślnie skonfigurowano terminarz uruchamiania zadania codziennie o godzinie 01:00 z automatyczną randomizacją i wyłączoną opcją **Uruchom pominięte zadania**.

Jeśli reguły obowiązujące w organizacji nakazują wyłączanie urządzeń na noc, zadanie instalacji uaktualnień nigdy nie zostanie uruchomione. Terminarz dla zadania wykrywania luk należy skonfigurować w oparciu o zasady obowiązujące w organizacji. Należy pamiętać, że zadanie instalacji uaktualnień może wymagać ponownego uruchomienia urządzenia.

Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji

Struktura grup administracyjnych w Kaspersky Security Center pełni następujące funkcje:

- Tworzy zakres profili.

  Istnieje alternatywny sposób stosowania odpowiednich ustawień na urządzeniach przy użyciu profili zasad. W tym przypadku zakres profili jest tworzony ze znacznikami, lokalizacjami urządzeń w jednostkach organizacyjnych Active Directory, członkostwem w grupach zabezpieczeń Active Directory itd.

- Tworzy zakres zadań grupowych.

  Istnieje sposób określania zakresu zadań grupowych, który nie jest oparty na hierarchii grup administracyjnych: korzystanie z zadań dla wyboru urządzeń oraz z zadań dla wskazanych urządzeń.

- Nadaje urządzeniom, wirtualnym Serwerom administracyjnym oraz podrzędnym Serwerom administracyjnym prawa dostępu.

- Przypisuje punkty dystrybucji.

Podczas tworzenia struktury grup administracyjnych należy wziąć pod uwagę topologię sieci organizacji dla optymalnego przydzielenia punktów dystrybucji. Optymalne przydzielenie punktów dystrybucji pozwala na zmniejszenie ruchu w sieci organizacji.

W zależności od schematu organizacyjnego oraz topologii sieci zaadaptowanej przez klienta MSP, w strukturze grup administracyjnych można zastosować następujące standardowe konfiguracje:

- Jedno biuro

- Wiele małych, oddzielonych od siebie biur

Standardowa konfiguracja klienta MSP: Jedno biuro

W standardowej konfiguracji „jedno biuro" wszystkie urządzenia znajdują się w obrębie sieci organizacji i są dla siebie widoczne. Sieć organizacji może zawierać kilka oddzielnych części (sieci lub fragmentów sieci) połączonych ze sobą wąskimi kanałami.

Dostępne są następujące metody tworzenia struktury grup administracyjnych:

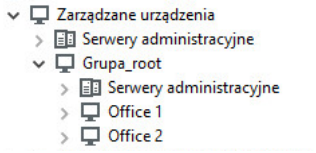
- Tworzenie struktury grup administracyjnych z uwzględnieniem topologii sieci. Struktura grup administracyjnych nie musi odzwierciedlać topologii sieci z absolutną dokładnością. Wystarczy dopasowanie oddzielnych części sieci i pewnych grup administracyjnych. Możesz skorzystać z automatycznego przydzielenia punktów dystrybucji lub zrobić to ręcznie.

- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie punktów dystrybucji, a następnie wskazać jedno lub kilka urządzeń jako punkty dystrybucji dla głównej grupy administracyjnej w każdej z oddzielnych części sieci, na przykład dla grupy **Zarządzane urządzenia**. Wszystkie punkty dystrybucji będą na tym samym poziomie i będą obejmować ten sam obszar, uwzględniając wszystkie urządzenia w sieci organizacji. W takim przypadku każdy z Agentów sieciowych połączy się z punktem dystrybucji o najkrótszej trasie. Trasę do punktu dystrybucji można ustalić za pomocą narzędzia tracert.

Standardowa konfiguracja klienta MSP: Wiele małych, zdalnych biur

Ta standardowa konfiguracja została utworzona z myślą o małych zdalnych biurach, które mogą kontaktować się z główną siedzibą za pośrednictwem Internetu. Każde zdalne biuro znajduje się poza NAT, czyli połączenie jednego zdalnego biura z innym jest niemożliwe, gdyż biura są od siebie odizolowane.

Konfiguracja musi być odzwierciedlona w strukturze grup administracyjnych: dla każdego zdalnego biura musi zostać utworzona oddzielna grupa administracyjna (grupy **Office 1** i **Office 2** na rysunku poniżej).



Zdalne biura uwzględnione w strukturze grupy administracyjnej

Do każdej grupy administracyjnej odpowiadającej biuru należy przydzielić jeden lub kilka punktów dystrybucji. Punktami dystrybucji muszą być urządzenia w zdalnym biurze, które posiadają wystarczającą ilość wolnego miejsca na dysku. Urządzenia z grupy **Office 1** będą, na przykład, łączyć się z punktami dystrybucji przydzielonymi do grupy administracyjnej **Office 1**.

Jeśli niektórzy użytkownicy poruszają się między biurami ze swoimi laptopami, w każdym zdalnym biurze, dla grupy administracyjnej najwyższego poziomu (**Główna grupa dla biur** na poniższym rysunku) należy wskazać dwa lub więcej urządzeń jako punkty dystrybucji (oprócz już istniejących punktów dystrybucji).

Na przykład: Laptop znajduje się w grupie administracyjnej **Office 1**, a następnie zostaje fizycznie przeniesiony do biura, które odpowiada grupie administracyjnej **Office 2**. Po przeniesieniu laptopa, Agent sieciowy spróbuje połączyć się z punktami dystrybucji przypisanymi do grupy **Office 1**, ale te punkty dystrybucji są niedostępne. Następnie Agent sieciowy próbuje połączyć się z punktami dystrybucji, które zostały przypisane do **Głównej grupy dla biur**. Ponieważ zdalne biura są odizolowane od siebie, próby nawiązania połączenia z punktami dystrybucji przypisanymi do grupy administracyjnej **Główna grupa dla biur** zakończą się pomyślnie tylko wtedy, gdy Agent sieciowy spróbuje połączyć się z punktami dystrybucji w grupie **Office 2**. Oznacza to, że laptop pozostanie w grupie administracyjnej, która odpowiada pierwszemu biuru, ale będzie korzystał z punktu dystrybucji biura, w którym aktualnie się znajduje.

Hierarchia profili i korzystanie z profili

W tej sekcji można znaleźć informacje dotyczące stosowania profili do urządzeń w grupach administracyjnych. Ta sekcja zawiera również informacje o profilach zasad.

Hierarchia profili

W Kaspersky Security Center profile są używane do określenia jednego zestawu ustawień dla kilku urządzeń. Na przykład, obszar profilu aplikacji P zdefiniowanej dla grupy administracyjnej G zawiera zarządzane urządzenia z zainstalowaną aplikacją P, które zostały dodane do grupy G i wszystkich jej podgrup, za wyjątkiem podgrup, we właściwościach których odznaczono opcję **Dziedzicz z grupy nadrzędnej**.

Profil można odróżnić od lokalnego ustawienia po ikonach kłódki (🔒) obok jego ustawień. Jeśli ustawienie (lub grupa ustawień) jest zablokowane we właściwościach zasady, w pierwszej kolejności należy użyć tego ustawienia (lub grupy ustawień) podczas tworzenia obowiązującego ustawienia, a następnie należy zapisać ustawienie (lub grupę ustawień) do zasady podrzędnej.

Tworzenie obowiązujących ustawień można opisać w następujący sposób: wartości wszystkich ustawień, które nie zostały zablokowane, są kopiowane z profilu, a następnie są nadpisywane przez wartości ustawień lokalnych, a w kolejnym etapie wartości wynikowe są nadpisywane przez zablokowane ustawienia pobrane z profilu.

Profile tej samej aplikacji oddziałują na siebie poprzez hierarchię grup administracyjnych: Zablokowane ustawienia z profilu nadrzędnego nadpisują te same ustawienia z profilu podrzędnego.

Dla użytkowników mobilnych istnieje specjalny profil. Ten profil jest aktywowany na urządzeniu, gdy to przełącza się do trybu użytkownika mobilnego. Zasady użytkowników mobilnych nie oddziałują na inne zasady poprzez hierarchię grup administracyjnych.

> Profil użytkownika mobilnego nie będzie obsługiwany w kolejnych wersjach Kaspersky Security Center. Zamiast profili użytkowników mobilnych będą używane profile zasad.

Profile zasad

Stosowanie profili na urządzeniach tylko poprzez hierarchię grup administracyjnych może być niewygodne tylko w kilku przypadkach. Konieczne może być utworzenie kilku instancji jednego profilu, które różnią się jednym lub dwoma ustawieniami dla różnych grup administracyjnych, oraz zsynchronizowanie zawartości tych profili w przyszłości.

Aby uniknąć takich problemów, Kaspersky Security Center obsługuje *profile zasad*. Profil zasad jest to inaczej podzbiór ustawień profilu. Ten podzbiór jest stosowany na urządzeniach docelowych wraz z profilem i uzupełnia go zgodnie z określonym warunkiem zwanym *warunkiem aktywacji profilu*. Profile mogą zawierać tylko ustawienia różniące się od "podstawowego" profilu, który jest aktywny na urządzeniu klienckim (komputerze lub urządzeniu mobilnym). Aktywacja profilu zmodyfikuje ustawienia zasad, które były aktywne na urządzeniu przed aktywacją profilu. Te ustawienia przyjmują wartości określone w profilu.

Aktualnie na profile zasad nałożone są następujące ograniczenia:

- Profil może zawierać maksymalnie 100 profili.
- Profil zasad nie może zawierać innych profili.
- Profil zasad nie może zawierać ustawień powiadamiania.

Zawartość profilu

Profil zasad zawiera następujące elementy:

- Profile z takimi samymi nazwami wpływają na siebie poprzez hierarchię grup administracyjnych ze wspólnymi regułami.
- Podzbiór ustawień profilu. Profil zawiera tylko aktualnie wymagane ustawienia (ustawienia zablokowane).
- Warunek aktywacji to wyrażenie logiczne z właściwościami urządzenia. Profil jest aktywny (uzupełnia zasadę) tylko wtedy, gdy warunek aktywacji profilu jest prawdziwy. We wszystkich pozostałych przypadkach profil jest nieaktywny i jest ignorowany. W wyrażeniu logicznym mogą być uwzględnione następujące właściwości urządzenia:
  - Stan trybu użytkownika mobilnego.
  - Właściwości środowiska sieciowego — nazwa aktywnej reguły dla połączenia z Agentem sieciowym.
  - Obecność lub brak określonych znaczników na urządzeniu.
  - Lokalizacja urządzenia w jednostce Active Directory: jawna (urządzenie znajduje się w określonej jednostce OU) lub niejawna (urządzenie jest w jednostce OU, która znajduje się w określonej jednostce OU na dowolnym poziomie zagnieżdżenia).
  - Członkostwo urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).
  - Członkostwo właściciela urządzenia w grupie zabezpieczeń Active Directory (jawne lub niejawne).
- Pole wyłączające profil. Wyłączone profile są zawsze ignorowane, a ich odpowiednie warunki aktywacji nie są sprawdzane.
- Priorytet profilu. Warunki aktywacji różnych profili są niezależne, a więc można aktywować kilka profili jednocześnie. Jeśli aktywne profile zawierają nienakładające się na siebie zbiory ustawień, nie pojawi się żaden problem. Jednakże dwa aktywne profile zawierające różne wartości tego samego ustawienia spowodują niejednoznaczność. Tę niejednoznaczność można wyeliminować poprzez priorytety profilu: Wartość niejednoznacznej zmiennej zostanie pobrana z profilu, który ma wyższy priorytet (ten, który znajduje się wyżej na liście profili).

Zachowanie profili, gdy zasady oddziałują na siebie poprzez hierarchię

Profile o tych samych nazwach zostają scalone zgodnie z regułami scalania profilu. Profile zasady nadrzędnej mają wyższy priorytet niż zasady podrzędnej. Jeśli modyfikowanie ustawień jest zabronione w zasadzie nadrzędnej (są zablokowane), zasada podrzędna używa warunków aktywacji profilu z zasady nadrzędnej. Jeśli modyfikowanie ustawień jest dozwolone w zasadzie nadrzędnej, używane są warunki aktywacji profilu z zasady podrzędnej.

Ponieważ w swoim warunku aktywacji profil zasad może zawierać opcję **Urządzenie jest w trybie offline**, profile całkowicie zastępują funkcję profili dla użytkowników mobilnych, które nie będą już obsługiwane.

Profil dla użytkowników mobilnych może zawierać profile, ale te profile mogą zostać aktywowane dopiero po przełączeniu urządzenia w tryb użytkownika mobilnego.

Zadania

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

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

Zadania mogą być wykonywane na Serwerze administracyjnym i na urządzeniach.

Na Serwerze administracyjnym wykonywane są następujące zadania:

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

Na urządzeniach wykonywane są następujące typy zadań:

- *Zadania lokalne*—zadania wykonywane na określonym urządzeniu

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

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

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

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

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

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

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

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

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

Reguły przenoszenia urządzeń

Zalecane jest automatyczne przydzielenie urządzeń do grup administracyjnych na serwerze wirtualnym, odpowiadającemu klientowi MSP, przy użyciu *reguł przenoszenia urządzeń*. Reguła przenoszenia urządzeń składa się z trzech głównych części: nazwy, warunku wykonania (wyrażenie logiczne z atrybutami urządzenia) oraz docelowej grupy administracyjnej. Reguła przenosi urządzenie do docelowej grupy administracyjnej, jeśli atrybuty urządzenia spełniają warunek wykonania reguły.

Wszystkie reguły przenoszenia urządzeń posiadają priorytety. Serwer administracyjny sprawdza, czy atrybuty urządzenia spełniają warunek wykonania każdej reguły, w rosnącej kolejności priorytetów. Jeśli atrybuty urządzenia spełniają warunek wykonania reguły, urządzenie zostaje przeniesione do grupy docelowej, a przetwarzanie reguły zostanie zakończone dla tego urządzenia. Jeśli atrybuty urządzenia spełniają warunki kilku reguł, urządzenie zostanie przeniesione do grupy docelowej reguły z najwyższym priorytetem (czyli tej, która znajduje się najwyżej na liście).

Reguły przenoszenia urządzeń mogą być tworzone pośrednio. Na przykład, we właściwościach pakietu instalacyjnego lub zadania zdalnej instalacji możesz określić grupę administracyjną, do której urządzenie musi zostać przeniesione po zainstalowaniu na nim Agenta sieciowego. Reguły przenoszenia urządzeń mogą być tworzone także bezpośrednio przez administratora Kaspersky Security Center na liście reguł przenoszenia. Lista ta znajduje się w Konsoli administracyjnej, we właściwościach grupy **Urządzenia nieprzypisane**.

Domyślnie reguła przenoszenia urządzeń jest przeznaczona do jednorazowego, wstępnego przydzielenia urządzeń do grup administracyjnych. Reguła przenosi urządzenia z grupy **Urządzenia nieprzypisane** tylko raz. Jeśli urządzenie był już raz przeniesione przy użyciu tej reguły, reguła ta nie przeniesie go już nawet wtedy, gdy ręcznie przeniesiesz urządzenie z powrotem do grupy **Urządzenia nieprzypisane**. Jest to zalecany sposób stosowania reguł przenoszenia.

Możesz przenieść urządzenia, które już zostały przydzielone do niektórych grup administracyjnych. W tym celu, we właściwościach reguły odznacz pole **Przenoś tylko urządzenia, które nie są przypisane do grup administracyjnych**.

Stosowanie reguł przenoszenia do urządzeń, które już zostały przydzielone do niektórych grup administracyjnych, znacząco zwiększa obciążenie na Serwerze administracyjnym.

Możesz utworzyć regułę przenoszenia, która będzie nieprzerwanie oddziaływać na jedno urządzenie.

Szczególnie zalecane jest unikanie ciągłego przenoszenia jednego urządzenia z jednej grupy do drugiej (na przykład, w celu zastosowania specjalnego profilu do tego urządzenia, uruchomienia specjalnego zadania grupowego lub zaktualizowania urządzenia poprzez punkt dystrybucji).

Takie scenariusze nie są obsługiwane, ponieważ w bardzo dużym stopniu zwiększają obciążenie na Serwerze administracyjnym oraz ruch sieciowy. Te scenariusze doprowadzają też do konfliktu z zasadami działania Kaspersky Security Center (szczególnie w obszarze uprawnień dostępu, zdarzeń i raportów). Należy znaleźć inne rozwiązanie, na przykład, poprzez użycie profili zasad, zadań dla wyborów urządzeń, przydzielania Agentów sieciowych zgodnie ze standardowym scenariuszem itd.

Kategoryzacja oprogramowania

Głównym narzędziem do monitorowania uruchomień aplikacji są *kategorie Kaspersky* (zwane dalej *Kategorie KL*). Kategorie KL umożliwiają administratorom Kaspersky Security Center uproszczenie obsługi kategoryzacji oprogramowania i zminimalizowanie ruchu sieciowego skierowanego do zarządzanych urządzeń.

Kategorie użytkownika powinny być tworzone tylko dla aplikacji, których nie można zaklasyfikować do żadnej z istniejących kategorii KL (na przykład, dla oprogramowania wykonanego na zamówienie użytkownika). Kategorie użytkownika są tworzone na podstawie pakietu instalacyjnego aplikacji (MSI) lub folderu z pakietami instalacyjnymi.

Jeśli dostępna jest duża ilość programów, które nie zostały skategoryzowane poprzez kategorie KL, można utworzyć automatycznie aktualizowaną kategorię. Sumy kontrolne plików wykonywalnych będą automatycznie dodawane do tej kategorii po każdej modyfikacji folderu zawierającego pakiety dystrybucyjne.

Automatycznie aktualizowanych kategorii oprogramowania nie można tworzyć na podstawie folderów Moje dokumenty, %windir% oraz %ProgramFiles%. Pula plików w tych folderach podlega częstym zmianom, co prowadzi do zwiększonego obciążenia na Serwerze administracyjnym i zwiększonego ruchu sieciowego. Należy utworzyć dedykowany folder ze zbiorem oprogramowania i okresowo dodawać do niego nowe elementy.

Informacje o aplikacjach wielodostępowych

Kaspersky Security Center umożliwia administratorom dostawców usług i administratorom dzierżawy używanie aplikacji Kaspersky z obsługą wielodostępności. Po zainstalowaniu aplikacji wielodostępowej firmy Kaspersky w infrastrukturze dostawcy usługi, dzierżawcy mogą rozpocząć korzystanie z aplikacji.

Aby oddzielić zadania i profile dotyczące różnych dzierżawców, musisz utworzyć dedykowany wirtualny Serwer administracyjny w Kaspersky Security Center dla każdego dzierżawcy. Wszystkie zadania i profile dla aplikacji wielodostępowych uruchomionych dla dzierżawcy muszą zostać utworzone dla grupy administracyjnej Zarządzane urządzenia wirtualnego Serwera administracyjnego odpowiadającego temu dzierżawcy. Zadania utworzone dla grup administracyjnych dotyczących głównego Serwera administracyjnego nie wpływają na urządzenia dzierżawców.

W przeciwieństwie do administratorów dostawcy usługi, administrator dzierżawy może tworzyć i przeglądać zadania i profile aplikacji tylko dla urządzeń odpowiedniego dzierżawcy. Zestawy ustawień zadań i profili dostępne dla administratorów dostawcy usługi i administratorów dzierżawy różnią się między sobą. Niektóre zestawy ustawień zadań i profili nie są dostępne dla administratorów dzierżawy.

W obrębie hierarchicznej struktury dzierżawy profile utworzone dla aplikacji wielodostępowych są dziedziczone przez grupy administracyjne niższego poziomu, a także przez grupy administracyjne wyższego poziomu: profil jest przesyłany do wszystkich urządzeń klienckich, które należą do dzierżawcy.

Tworzenie kopii zapasowej i przywracanie ustawień Serwera administracyjnego

Tworzenie kopii zapasowej ustawień Serwera administracyjnego i jego baz danych odbywa się przy użyciu zadania tworzenia kopii zapasowej oraz narzędzia klbackup. Kopia zapasowa zawiera wszystkie główne ustawienia i obiekty dotyczące Serwera administracyjnego, takie jak certyfikaty, klucze główne do szyfrowania dysków na zarządzanych urządzeniach, klucze dla różnych licencji, strukturę grup administracyjnych z całą ich zawartością, zadaniami, zasadami itd. Przy pomocy kopii zapasowej można przywrócić działanie Serwera administracyjnego tak szybko, jak to możliwe, poświęcając na to od kilkunastu minut do kilku godzin.

Jeśli nie ma dostępnej kopii zapasowej, błąd może doprowadzić do bezpowrotnej utraty certyfikatów i wszystkich ustawień Serwera administracyjnego. Będzie to wymagało przeprowadzenia konfiguracji Kaspersky Security Center od początku oraz ponownego zainstalowania Agenta sieciowego w sieci organizacji. Wszystkie klucze główne do szyfrowania dysków na zarządzanych urządzeniach zostaną utracone, co spowoduje ryzyko utraty zaszyfrowanych danych na urządzeniach z zainstalowanym programem Kaspersky Endpoint Security. Dlatego też nigdy nie rezygnuj z regularnego wykonywania kopii zapasowej Serwera administracyjnego przy użyciu standardowego zadania tworzenia kopii zapasowej.

Kreator wstępnej konfiguracji tworzy zadanie wykonywania kopii zapasowej dla ustawień Serwera administracyjnego i ustawia jego codzienne wykonywanie na godzinę 4:00. Kopie zapasowe są domyślnie zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskySC.

Jeśli serwer Microsoft SQL Server, zainstalowany na innym urządzeniu, jest używany jako DBMS, należy zmodyfikować zadanie tworzenia kopii zapasowej, określając jako folder do przechowywania kopii zapasowych ścieżkę UNC, która jest używana do zapisywania usługi Serwera administracyjnego oraz usługi SQL Server. To wymaganie, które nie jest oczywiste, wynika ze specyfiki specjalnej funkcji kopii zapasowej w systemie DBMS serwera Microsoft SQL Server.

Jeśli jako system DBMS używana jest lokalna instancja serwera Microsoft SQL Server, zalecane jest zapisanie kopii zapasowych na dedykowanym nośniku w celu zabezpieczenia ich przed uszkodzeniem wraz z Serwerem administracyjnym.

Ponieważ kopia zapasowa zawiera ważne dane, zadanie tworzenia kopii zapasowej oraz narzędzie klbackup oferują ochronę kopii zapasowej przy użyciu hasła. Domyślnie zadanie tworzenia kopii zapasowej wykonuje kopię zapasową z pustym hasłem. Hasło należy ustawić we właściwościach zadania tworzenia kopii zapasowej. Pominięcie tego wymagania doprowadza do sytuacji, w której wszystkie klucze certyfikatów Serwera administracyjnego, klucze dla licencji oraz klucze główne dla szyfrowania dysków na zarządzanych urządzeniach pozostaną niezaszyfrowane.

Oprócz regularnych kopii zapasowych, kopie zapasowe należy tworzyć także przed każdą znaczącą zmianą, w tym instalacją aktualizacji i łat Serwera administracyjnego.

Jeśli używasz Microsoft SQL Server jako DBMS, możesz zminimalizować rozmiar kopii zapasowych. W tym celu włącz opcję **Kompresuj kopię zapasową** w ustawieniach SQL Server.

Przywracanie kopii zapasowej odbywa się przy użyciu narzędzia klbackup na działającej instancji Serwera administracyjnego, który został właśnie zainstalowany i posiada tę samą wersję (lub nowszą), dla której kopia zapasowa została utworzona.

Instancja Serwera administracyjnego, na którym kopia zapasowa ma zostać przywrócona, musi korzystać z systemu DBMS tego samego typu (na przykład ten sam SQL Server lub MariaDB) i tej samej lub nowszej wersji. Wersja Serwera administracyjnego może być taka sama (z tą samą lub późniejszą łatą) lub nowsza.

Sekcja opisuje standardowe scenariusze przywracania ustawień i obiektów Serwera administracyjnego.

Urządzenie z zainstalowanym Serwerem administracyjnym nie działa

Jeśli urządzenie, na którym jest zainstalowany Serwer administracyjny, nie działa z powodu błędu, zalecane jest wykonanie następujących działań:

- Nowy Serwer administracyjny musi posiadać ten sam adres: nazwę NetBIOS, nazwę FQDN lub statyczny adres IP (w zależności od tego, co zostało ustawione podczas instalacji Agentów sieciowych).
- Zainstaluj Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.
- W menu **Start** uruchom narzędzie klbackup i wykonaj przywracanie.

Ustawienia Serwera administracyjnego lub bazy danych są uszkodzone

Jeżeli Serwer administracyjny nie działa ze względu na uszkodzone ustawienia lub bazę danych (na przykład, w wyniku przepięcia), zalecane jest użycie następujących scenariuszy:

1. Przeskanuj system plików na uszkodzonym urządzeniu.
2. Odinstaluj niedziałającą wersję Systemu operacyjnego.
3. Zainstaluj ponownie Serwer administracyjny, używając systemu DBMS tego samego typu i w tej samej (lub nowszej) wersji. Możesz zainstalować tę samą wersję Serwera z tą samą (lub późniejszą) łatą lub nowszą wersję Serwera. Po instalacji nie przeprowadzaj wstępnej konfiguracji przy użyciu kreatora.
4. Z poziomu menu **Start** uruchom narzędzie klbackup i przywróć kopię zapasową.

Zabronione jest przywracanie Serwera administracyjnego w sposób inny niż przy użyciu narzędzia klbackup.

Wszelkie próby przywrócenia Serwera administracyjnego przy użyciu oprogramowania firm trzecich doprowadzą do desynchronizacji danych na węzłach aplikacji Kaspersky Security Center i w konsekwencji - do niepoprawnego działania aplikacji.

Instalowanie Agenta sieciowego i aplikacji zabezpieczającej

Aby zarządzać urządzeniami w organizacji, na każdym z nich należy zainstalować Agenta sieciowego. Zdalna instalacja aplikacji Kaspersky Security Center na urządzeniach w firmie zazwyczaj rozpoczyna się od zainstalowania na nich Agenta sieciowego.

W systemie Microsoft Windows XP Agent sieciowy może nie wykonać poprawnie następujących działań: pobranie uaktualnień bezpośrednio z serwerów Kaspersky (jako punkt dystrybucji); działanie jako serwer proxy KSN (jako punkt dystrybucji); oraz wykrywanie luk firm trzecich (jeśli używane jest Zarządzanie lukami i poprawkami).

Wstępna zdalna instalacja

Jeśli Agent sieciowy został już zainstalowany na urządzeniu, zdalna instalacja aplikacji na tym urządzeniu odbywa się poprzez Agenta sieciowego. Pakiet dystrybucyjny aplikacji, która ma zostać zainstalowana, jest przesyłany za pośrednictwem kanałów komunikacji pomiędzy Agentami sieciowymi i Serwerem administracyjnym wraz z ustawieniami instalacji, zdefiniowanymi przez administratora. Aby przesłać pakiet dystrybucyjny, możesz użyć węzłów pośredniczących, na przykład, punktów dystrybucji, dostarczania multiemisyjnego itd. Więcej informacji dotyczących instalacji aplikacji na zarządzanych urządzeniach, na których jest już zainstalowany Agent sieciowy, można znaleźć poniżej.

Możesz przeprowadzić wstępną instalację Agenta sieciowego na urządzeniach działających pod kontrolą systemu Windows, korzystając z jednej z następujących metod:

- Używając narzędzi firm trzecich do zdalnej instalacji aplikacji.
- Korzystając z zasad grupy w systemie Windows: używając standardowych narzędzi do zarządzania systemu Windows dla zasad grupy.
- W trybie wymuszonym, korzystając ze specjalnych opcji w zadaniu zdalnej instalacji programu Kaspersky Security Center.
- Wysyłając do użytkowników urządzeń odnośniki do pakietów autonomicznych, wygenerowanych przez Kaspersky Security Center. Pakiety autonomiczne to moduły wykonywalne, które zawierają pakiety dystrybucyjne wybranych aplikacji wraz ze zdefiniowanymi ustawieniami.
- Ręcznie, poprzez uruchomienie instalatorów aplikacji na urządzeniach.

Na platformach innych niż Microsoft Windows należy przeprowadzić wstępną instalację Agenta sieciowego na zarządzanych urządzeniach przy użyciu istniejących narzędzi firm trzecich lub ręcznie, poprzez wysłanie do użytkowników archiwów ze wstępnie skonfigurowanym pakietem dystrybucyjnym. Na platformach innych niż Windows możesz uaktualnić Agenta sieciowego do nowej wersji lub zainstalować inne aplikacje firmy Kaspersky, korzystając z Agentów sieciowych (już zainstalowanych na urządzeniach) przeznaczonych do wykonywania zadań zdalnej instalacji. W tym przypadku instalacja przebiega identycznie jak instalacja na urządzeniach działających pod kontrolą systemu Microsoft Windows.

Podczas wybierania metody i strategii zdalnej instalacji aplikacji w zarządzanej sieci należy mieć na uwadze kilka czynników (częściowa lista):

- Konfiguracja sieci korporacyjnej.
- Całkowitą liczbę urządzeń.
- Obecność domen Windows w zarządzanej sieci, możliwość modyfikacji profili grup Active Directory w tych domenach.
- Wykrywanie kont użytkowników z uprawnieniami lokalnego administratora na urządzeniach, na których została zaplanowana wstępna zdalna instalacja aplikacji firmy Kaspersky (dostępność konta użytkownika domeny z

uprawnieniami lokalnego administratora lub obecność ujednoliconych lokalnych kont użytkowników z uprawnieniami administratora na tych urządzeniach).

- Typ połączenia i przepustowość kanału sieciowego pomiędzy Serwerem administracyjnym a sieciami klienckimi MSP, a także przepustowość kanałów w tych sieciach.

- Ustawienia zabezpieczeń zastosowane na zdalnych urządzeniach w momencie uruchomienia zdalnej instalacji (na przykład, użycie UAC lub Prostego udostępniania plików).

Konfigurowanie instalatorów

Przed uruchomieniem zdalnej instalacji aplikacji Kaspersky w sieci, należy określić ustawienia instalacji (ustawienia definiowane podczas instalacji aplikacji). Podczas instalacji Agenta sieciowego należy określić przynajmniej adres połączenia z Serwerem administracyjnym i ustawienia proxy; niektóre ustawienia zaawansowane też mogą być wymagane. W zależności od wybranej metody instalacji, ustawienia można zdefiniować w różny sposób. W najprostszym przypadku (ręczna interaktywna instalacja na wybranym urządzeniu) wszystkie odpowiednie ustawienia można zdefiniować w interfejsie instalatora, co oznacza, że w niektórych sytuacjach wstępna instalacja może być wykonana nawet poprzez wysłanie do użytkownika odnośnika do pakietu dystrybucyjnego Agenta sieciowego wraz z ustawieniami (adres Serwera administracyjnego itd.), które użytkownik powinien wprowadzić w interfejsie instalatora.

Ta metoda nie jest zalecana, gdyż jest ona niewygodna dla użytkowników, ponieważ stwarza duże ryzyko występowania błędów podczas ręcznego definiowania ustawień; nie można jej używać podczas nieinteraktywnej cichej instalacji aplikacji w grupie urządzeń. Na ogół administrator musi określić wartości dla ustawień w sposób scentralizowany; te wartości mogą być następnie użyte podczas tworzenia pakietów autonomicznych. Pakiety autonomiczne to samorozpakowujące się archiwa, które zawierają pakiety dystrybucyjne z ustawieniami zdefiniowanymi przez administratora. Pakiety autonomiczne mogą znajdować się w zasobach, z których mogą pobierać użytkownicy końcowi (na przykład, na serwerze Kaspersky Security Center Web Server) i które umożliwiają przeprowadzenie instalacji nieinteraktywnej na wybranych urządzeniach w sieci.

Pakiety instalacyjne

Pierwsza i główna metoda definiowania ustawień instalacji aplikacji jest uniwersalna i tym samym jest odpowiednia dla wszystkich metod instalacji: przy użyciu narzędzi Kaspersky Security Center oraz większości narzędzi firm trzecich. Ta metoda obejmuje utworzenie pakietów instalacyjnych aplikacji w Kaspersky Security Center.

Pakiety instalacyjne są generowane przy użyciu następujących metod:

- Automatycznie, z określonych pakietów dystrybucyjnych, na podstawie załączonych *deskryptorów* (pliki z rozszerzeniem .kud, które zawierają reguły dla instalacji, wyniki analizy oraz inne informacje)

- Z plików wykonywalnych instalatorów lub z instalatorów w formacie Microsoft Windows Installer (MSI), które są dla standardowych lub obsługiwanych aplikacji

Wygenerowane pakiety instalacyjne są zorganizowane hierarchicznie jako foldery z podfolderami i plikami. Oprócz oryginalnego pakietu dystrybucyjnego, pakiet instalacyjny zawiera ustawienia dostępne do modyfikacji (w tym ustawienia instalatora oraz reguły przetwarzania dla takich sytuacji, jak konieczność ponownego uruchomienia systemu operacyjnego w celu zakończenia instalacji), a także drobne moduły pomocnicze.

Wartości ustawień instalacji, które są określone dla wybranej obsługiwanej aplikacji, można zdefiniować w interfejsie Konsoli administracyjnej podczas tworzenia pakietu instalacyjnego (więcej ustawień można znaleźć we właściwościach już utworzonego pakietu instalacyjnego). Podczas zdalnej instalacji aplikacji przy użyciu narzędzi Kaspersky Security Center pakiety instalacyjne są dostarczane na urządzenia docelowe, dzięki czemu uruchomienie instalatora aplikacji udostępni dla tej aplikacji wszystkie ustawienia zdefiniowane przez administratora. Jeśli do zainstalowania aplikacji firmy Kaspersky używasz narzędzi firm trzecich, musisz zapewnić dostępność całego pakietu instalacyjnego na urządzeniu docelowym, czyli pakietu dystrybucyjnego i jego ustawień. Pakiety instalacyjne są tworzone i przechowywane przez Kaspersky Security Center w dedykowanym podfolderze udostępnionego folderu danych.

W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.

Instrukcje dotyczące korzystania z tej metody konfiguracji dla aplikacji Kaspersky przed ich zainstalowaniem przy użyciu narzędzi firm trzecich można znaleźć w sekcji „Zdalna instalacja przy użyciu zasad grupy Microsoft Windows".

Natychmiast po zainstalowaniu programu Kaspersky Security Center, automatycznie zostaje wygenerowanych kilka pakietów instalacyjnych. Pakiety te są gotowe do zainstalowania i zawierają pakiety Agenta sieciowego oraz pakiety aplikacji zabezpieczających dla Microsoft Windows.

W niektórych przypadkach używanie pakietów instalacyjnych do zdalnego instalowania aplikacji w sieci klienckiej MSP oznacza konieczność utworzenia pakietów instalacyjnych na Serwerach wirtualnych, które odpowiadają klientom MSP. Utworzenie pakietów instalacyjnych na Serwerach wirtualnych umożliwia użycie różnych ustawień instalacji dla różnych klientów MSP. W pierwszej instancji jest to przydatne podczas zarządzania pakietami instalacyjnymi Agentów sieciowych, gdyż Agenty sieciowe zainstalowane w sieciach różnych klientów MSP używają różnych adresów do nawiązywania połączenia z Serwerem administracyjnym. Adres połączenia określa Serwer, z którym łączy się Agent sieciowy.

Oprócz możliwości natychmiastowego utworzenia nowych pakietów instalacyjnych na wirtualnym Serwerze administracyjnym, główny tryb działania dla pakietów instalacyjnych na wirtualnych Serwerach administracyjnych to „rozesłanie" pakietów instalacyjnych z głównego Serwera administracyjnego do Serwerów wirtualnych. Możesz rozesłać wybrane (lub wszystkie) pakiety instalacyjne na wybrane wirtualne Serwery administracyjne (w tym wszystkie Serwery w obrębie wybranej grupy administracyjnej) przy użyciu odpowiedniego zadania Serwera administracyjnego. Dodatkowo, podczas tworzenia nowego wirtualnego Serwera administracyjnego możesz wybrać listę pakietów instalacyjnych głównego Serwera administracyjnego. Wybrane pakiety zostaną natychmiast rozesłane do nowo utworzonego wirtualnego Serwera administracyjnego.

Podczas rozsyłania pakietu instalacyjnego jego zawartość nie jest kopiowana w całości. Repozytorium plików na wirtualnym Serwerze administracyjnym, który odpowiada rozsyłanemu pakietowi instalacyjnemu, przechowuje tylko pliki z ustawieniami określonymi dla tego Serwera wirtualnego. Główna część pakietu instalacyjnego (w tym pakiet dystrybucyjny instalowanej aplikacji) pozostanie niezmieniona. Jest ona przechowywana tylko w repozytorium głównego Serwera administracyjnego. Umożliwia to drastyczne zwiększenie wydajności systemu i zmniejszenie wymaganej przestrzeni na dysku. Podczas zarządzania pakietami instalacyjnymi rozsyłanymi do wirtualnych Serwerów administracyjnych (czyli podczas uruchamiania zadań zdalnej instalacji lub tworzenia autonomicznych pakietów instalacyjnych) dane z oryginalnego pakietu instalacyjnego głównego Serwera administracyjnego zostają „scalone" z plikami ustawień, które odpowiadają pakietowi przesłanemu na wirtualny Serwer administracyjny.

Klucz licencyjny dla aplikacji może zostać określony we właściwościach pakietu instalacyjnego, ale zalecane jest unikanie tej metody dystrybucji licencji, ponieważ łatwo jest uzyskać dostęp do odczytu plików w folderze. Dla kluczy licencyjnych należy używać zadań automatycznego rozsyłania kluczy licencyjnych lub instalacji.

Właściwości MSI i pliki transformacji

Innym sposobem skonfigurowania instalacji na platformie Windows jest zdefiniowanie właściwości MSI i plików transformacji. Ta metoda może być używana podczas instalacji przy użyciu narzędzi firm trzecich przeznaczonych dla instalatorów w formacie Microsoft Installer, a także podczas instalacji poprzez zasady grupy systemu Windows przy użyciu standardowych narzędzi Microsoft lub narzędzi innych firm przeznaczonych do zarządzania zasadami grupy systemu Windows.

Zdalna instalacja przy użyciu narzędzi firm trzecich

Jeśli w organizacji dostępne są jakiekolwiek narzędzia do zdalnej instalacji aplikacji (na przykład, Microsoft System Center), wygodnym rozwiązaniem będzie przeprowadzenie wstępnej zdalnej instalacji przy użyciu tych narzędzi.

Należy wykonać następujące czynności:

- Wybierz metodę konfiguracji instalacji, która najbardziej odpowiada używanemu narzędziu do zdalnej instalacji.
- Zdefiniuj mechanizm synchronizacji pomiędzy modyfikacją ustawień pakietów instalacyjnych (poprzez interfejs Konsoli administracyjnej) a działaniem wybranych narzędzi firm trzecich, używanych do zdalnej instalacji aplikacji z pakietu instalacyjnego.

Informacje ogólne o zadaniach zdalnej instalacji w Kaspersky Security Center

Kaspersky Security Center oferuje szeroki zakres metod zdalnej instalacji aplikacji, które są zaimplementowane pod postacią zadań zdalnej instalacji. Możesz utworzyć zadanie zdalnej instalacji dla określonej grupy administracyjnej oraz dla wskazanych urządzeń lub wyboru urządzeń (takie zadania są wyświetlane w Konsoli administracyjnej, w folderze **Zadania**). Podczas tworzenia zadania możesz wybrać pakiety instalacyjne (Agenta sieciowego i / lub innej aplikacji), które zostaną zainstalowane w obrębie tego zadania, a także określić pewne ustawienia, które definiują metodę zdalnej instalacji.

Zadania dla grup administracyjnych dotyczą urządzeń znajdujących się w określonej grupie oraz wszystkich urządzeń we wszystkich podgrupach tej grupy administracyjnej. Zadanie obejmuje urządzenia podrzędnych Serwerów administracyjnych znajdujących się w grupie lub jej dowolnych podgrupach, jeśli odpowiednie ustawienie zostało włączone w zadaniu.

Zadania dla wskazanych urządzeń aktualizują listę urządzeń klienckich przy każdym uruchomieniu zgodnie z zawartością wyborów w momencie uruchomienia zadania. Jeśli wybór zawiera urządzenia, które zostały połączone z podrzędnymi Serwerami administracyjnymi, zadanie zostanie uruchomione także na tych urządzeniach.

Aby zapewnić pomyślne działanie zadania zdalnej instalacji na urządzeniach połączonych z podrzędnymi Serwerami administracyjnymi, należy użyć zadania dystrybucji do przekazania pakietów instalacyjnych używanych przez zadanie użytkownika do odpowiednich podrzędnych Serwerów administracyjnych.

Zdalna instalacja przy użyciu zasad grupy Microsoft Windows

Przeprowadzenie wstępnej instalacji Agentów sieciowych poprzez zasady grupy Microsoft Windows jest zalecane wtedy, gdy spełnione są następujące warunki:

- Urządzenie należy do domeny Active Directory.

- Dostęp do kontrolera domeny zostaje nadany z uprawnieniami administratora, dzięki czemu możliwe jest utworzenie i zmodyfikowanie zasad grupy Active Directory.
- Skonfigurowane pakiety instalacyjne można przenieść do sieci, w której znajdują się zarządzane urządzenia docelowe (do folderu współdzielonego, dostępnego do odczytu dla wszystkich urządzeń docelowych).
- Schemat zdalnej instalacji umożliwia zaczekanie na kolejne rutynowe ponowne uruchomienie urządzeń docelowych przed rozpoczęciem zdalnej instalacji Agentów sieciowych na tych urządzeniach (lub można wymusić zastosowanie na tych urządzeniach zasady grupy systemu Windows).

Ten schemat instalacji charakteryzuje się następującymi cechami:

- Pakiet dystrybucyjny aplikacji w formacie Microsoft Installer (pakiet MSI) znajduje się w folderze współdzielonym (folder, w którym konta SystemLokalny urządzeń docelowych mają uprawnienia do odczytu).
- W zasadzie grupy Active Directory, dla pakietu dystrybucyjnego tworzony jest obiekt instalacji.
- Obszar instalacji jest ustawiany poprzez określenie jednostki organizacyjnej (OU) i/lub grupy zabezpieczeń, która zawiera urządzenia docelowe.
- Następnym razem, gdy urządzenie docelowe zaloguje się do domeny (przed zalogowaniem się użytkowników do systemu), wszystkie zainstalowane aplikacje są sprawdzane pod kątem żądanej aplikacji. Jeśli żądana aplikacja nie zostanie odnaleziona, pakiet dystrybucyjny zostanie pobrany z zasobu określonego w zasadzie, a następnie zostanie zainstalowany.

Ten schemat zdalnej instalacji niesie za sobą korzyść, jaką jest instalowanie przypisanych aplikacji na urządzeniach docelowych podczas ładowania systemu operacyjnego, czyli nawet przed zalogowaniem się użytkownika do systemu. Nawet jeśli użytkownik, który nie ma wystarczających uprawnień, usunie aplikację, zostanie ona ponownie zainstalowana przy kolejnym uruchomieniu systemu operacyjnego. Wadą tego schematu wdrożenia jest fakt, że zmiany w zasadzie grupowej, które zostały wprowadzone przez administratora, nie zostaną zastosowane, aż do ponownego uruchomienia urządzenia (jeśli nie są używane narzędzia dodatkowe).

Zasady grupy można użyć do zainstalowania Agenta sieciowego oraz innych aplikacji, jeśli ich instalatory są w formacie Windows Installer.

Poza tym, jeśli wybierzesz tę metodę wdrożenia, musisz mieć na uwadze obciążenie zasobu plików, z którego pliki zostaną skopiowane na urządzenia docelowe po zastosowaniu zasad grupy systemu Windows. Musisz także wybrać metodę dostarczenia skonfigurowanego pakietu instalacyjnego do tego zasobu, a także metodę synchronizacji odpowiednich zmian w jego ustawieniach.

Zarządzanie zasadami Microsoft Windows przy użyciu zadania zdalnej instalacji z programu Kaspersky Security Center

Ta metoda zdalnej instalacji jest dostępna tylko wtedy, gdy dostęp do kontrolera domeny, który zawiera urządzenia docelowe, jest możliwy z poziomu urządzenia z Serwerem administracyjnym, a także możliwy jest dostęp do odczytu folderu współdzielonego Serwera administracyjnego (tego, w którym znajdują się pakiety instalacyjne) z poziomu urządzeń docelowych. Ze względu na wyżej wspomniane przyczyny, ta metoda zdalnej instalacji nie jest stosowana do MSP.

Samodzielna instalacja aplikacji przy użyciu zasad Microsoft Windows

Administrator może tworzyć obiekty wymagane do zainstalowania w zasadach grupy systemu Windows w swoim imieniu. W tym przypadku pakiety należy przesłać na autonomiczny serwer plików i udostępnić odnośnik do nich.

Dostępne są następujące scenariusze instalacji:

- Administrator tworzy pakiet instalacyjny i konfiguruje jego ustawienia w Konsoli administracyjnej. Następnie administrator kopiuje cały podfolder EXEC tego pakietu z folderu współdzielonego Kaspersky Security Center do folderu w dedykowanym zasobie plików w organizacji. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w organizacji.

- Administrator pobiera pakiet dystrybucyjny aplikacji (w tym pakiet Agenta sieciowego) z Internetu i wysyła go do dedykowanego zasobu plików w organizacji. Obiekt zasad grupy zawiera odnośnik do pliku MSI tego pakietu, który jest przechowywany w podfolderze w dedykowanym zasobie plików w organizacji. Ustawienia instalacji są definiowane poprzez konfigurowanie właściwości MSI lub poprzez konfigurowanie plików transformacji MST.

Wymuszona zdalna instalacja przy użyciu zadania zdalnej instalacji z Kaspersky Security Center

Aby przeprowadzić wstępną zdalną instalację Agentów sieciowych lub innych aplikacji, należy wymusić instalację wybranych pakietów instalacyjnych przy użyciu zadania zdalnej instalacji programu Kaspersky Security Center—pod warunkiem, że każde urządzenie posiada konto użytkownika z uprawnieniami lokalnego administratora i przynajmniej jedno urządzenie z zainstalowanym Agentem sieciowym pełni rolę punktu dystrybucji w każdej podsieci.

W tej sytuacji możesz bezpośrednio wskazać urządzenia docelowe lub wybrać grupę administracyjną Kaspersky Security Center, do której należą, bądź też utworzyć wybór urządzeń w oparciu o określone kryterium. Instalacja rozpoczyna się zgodnie z terminarzem zadania. Jeśli we właściwościach zadania włączone jest ustawienie **Uruchom pominięte zadania**, zadanie może zostać uruchomione albo natychmiast po włączeniu urządzeń docelowych, albo po ich przeniesieniu do docelowej grupy administracyjnej.

Wymuszona instalacja obejmuje dostarczenie pakietów instalacyjnych do punktów dystrybucji, skopiowanie plików do zasobu admin$ na każdym urządzeniu docelowym, a także zdalną rejestrację usług pomocniczych na tych urządzeniach. Dostarczenie pakietów instalacyjnych do punktów dystrybucji odbywa się poprzez funkcję Kaspersky Security Center zapewniającą interakcję z siecią. W tym przypadku muszą być spełnione następujące warunki:

- Urządzenia docelowe są dostępne po stronie punktu dystrybucji.

- Rozwiązywanie nazw urządzeń docelowych działa poprawnie w sieci.

- Zasób administracyjny (admin$) pozostanie włączony na urządzeniach docelowych.

- Na urządzeniach docelowych jest uruchomiona usługa systemowa Serwer (domyślnie jest uruchomiona).

- W celu zezwolenia na zdalny dostęp przy użyciu narzędzi systemu Windows, na urządzeniach docelowych są otwarte poniższe porty: TCP 139, TCP 445, UDP 137 i UDP 138.

- Na urządzeniach docelowych z systemem Microsoft Windows XP tryb Proste udostępnianie plików jest wyłączony.

- Na urządzeniach docelowych udostępnianie i model zabezpieczeń są ustawione na *Klasyczny - uwierzytelnianie użytkowników lokalnych jako samych siebie*. W żadnym wypadku nie może być ustawione *Tylko gość - uwierzytelnianie użytkowników lokalnych jako gościa*.

- Urządzenia docelowe są członkami domeny lub wcześniej są tworzone na urządzeniach docelowych jednakowe konta z uprawnieniami administratora.

Urządzenia w grupach roboczych mogą zostać przystosowane zgodnie z powyższymi wymaganiami przy użyciu narzędzia riprep.exe, którego opis znajduje się na stronie działu pomocy technicznej firmy Kaspersky.

Podczas instalacji na nowych urządzeniach, które jeszcze nie zostały przydzielone do żadnej grupy administracyjnej Kaspersky Security Center, możesz otworzyć właściwości zadania zdalnej instalacji i określić grupę administracyjną, do której urządzenia zostaną przeniesione po zakończeniu instalacji Agenta sieciowego.

Podczas tworzenia zadania grupowego należy pamiętać, że każde zadanie grupowe ma wpływ na wszystkie urządzenia we wszystkich grupach zagnieżdżonych w wybranej grupie. Dlatego też należy unikać powielania zadań instalacji w podgrupach.

Automatyczna instalacja jest uproszczonym sposobem tworzenia zadań dla wymuszonej instalacji aplikacji. We właściwościach grupy administracyjnej należy otworzyć listę pakietów instalacyjnych i wybrać te, które muszą zostać zainstalowane na urządzeniach w tej grupie. W rezultacie, wybrane pakiety instalacyjne zostaną automatycznie zainstalowane na wszystkich urządzeniach w tej grupie i wszystkich jej podgrupach. Przedział czasu, w trakcie którego pakiety zostaną zainstalowane, zależy od przepustowości sieci i całkowitej liczby urządzeń w sieci.

Aby zezwolić na instalację wymuszoną, należy upewnić się, że w każdej odizolowanej podsieci zawierającej urządzenia docelowe znajdują się punkty dystrybucji.

Należy zauważyć, że ta metoda instalacji powoduje duże obciążenie urządzeń pełniących role punktów dystrybucji. Dlatego też zalecane jest wybranie jako punktów dystrybucji mocniejszych urządzeń z jednostkami przechowywania danych o wysokim poziomie wydajności. Co więcej, wolna przestrzeń na dysku, na którym znajduje się folder *%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit*, musi wielokrotnie przekraczać całkowity rozmiar pakietów dystrybucyjnych instalowanych aplikacji.

Uruchamianie pakietów autonomicznych utworzonych przez Kaspersky Security Center

Powyżej opisane metody wstępnej zdalnej instalacji Agenta sieciowego i innych aplikacji nie zawsze będą mogły zostać zaimplementowane, gdyż nie jest możliwe spełnienie wszystkich wymaganych warunków. W takich przypadkach można utworzyć standardowy plik wykonywalny zwany *autonomicznym pakietem instalacyjnym* poprzez Kaspersky Security Center, korzystając z pakietów instalacyjnych z odpowiednimi ustawieniami instalacji, które zostały przygotowane przez administratora. Autonomiczny pakiet instalacyjny może zostać opublikowany na wewnętrznym serwerze WWW (znajdującym się w Kaspersky Security Center), jeśli będzie to uzasadnione (zewnętrzny dostęp do tego serwera WWW został skonfigurowany dla użytkowników urządzeń docelowych), lub na specjalnie wdrożonym serwerze WWW znajdującym się w Kaspersky Security Center Web Console. Możesz także skopiować pakiety autonomiczne na inny serwer WWW.

Korzystając z Kaspersky Security Center, możesz wysłać do wybranych użytkowników wiadomość e-mail zawierającą odnośnik do pliku pakietu autonomicznego na aktualnie używanym serwerze WWW oraz prośbę o jego uruchomienie (w trybie interaktywnym lub z przełącznikiem "-s" dla cichej instalacji). Do wiadomości e-mail możesz załączyć autonomiczny pakiet instalacyjny, a następnie wysłać ją do użytkowników urządzeń, którzy nie mają dostępu do serwera WWW. Administrator może także skopiować pakiet autonomiczny na urządzenie zewnętrzne, dostarczyć go na odpowiednie urządzenie, a następnie uruchomić go.

Pakiet autonomiczny można utworzyć z pakietu Agenta sieciowego, pakietu innej aplikacji (na przykład, zabezpieczającej) lub z obu pakietów. Jeśli pakiet autonomiczny został utworzony z pakietu Agenta sieciowego i innej aplikacji, instalacja rozpocznie się z Agenta sieciowego.

Podczas tworzenia pakietu autonomicznego z pakietu Agenta sieciowego możesz określić grupę administracyjną, do której nowe urządzenia (te, które nie zostały przydzielone do żadnej grup administracyjnych) zostaną automatycznie przeniesione po zakończeniu instalacji Agenta sieciowego na tych urządzeniach.

Pakiety autonomiczne mogą być uruchomione w trybie interaktywnym (opcja domyślna), wyświetlając wynik instalacji aplikacji, które zawierają, lub mogą być uruchomione w trybie cichym (z przełącznikiem "-s"). Tryb cichy może zostać użyty dla instalacji ze skryptów, na przykład, ze skryptów skonfigurowanych do uruchamiania po wdrożeniu obrazu systemu operacyjnego. Wynik instalacji w trybie cichym jest determinowany przez kod zwrotny procesu.

Opcje ręcznej instalacji aplikacji

Administratorzy lub doświadczeni użytkownicy mogą zainstalować aplikacje ręcznie w trybie interaktywnym. Mogą oni użyć oryginalnych pakietów dystrybucyjnych lub wygenerowanych z nich pakietów instalacyjnych, które są przechowywane w folderze współdzielonym Kaspersky Security Center. Domyślnie instalatory są uruchamiane w trybie interaktywnym i wyświetlają użytkownikom komunikaty z pytaniami o podanie wszystkich wymaganych wartości. Jednakże podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego z przełącznikiem "-s", instalator zostanie uruchomiony w trybie cichym i z ustawieniami, które zostały określone podczas konfiguracji pakietu instalacyjnego.

Podczas uruchamiania procesu setup.exe z katalogu głównego pakietu instalacyjnego, pakiet zostanie najpierw skopiowany do tymczasowego folderu lokalnego, a następnie instalator aplikacji zostanie uruchomiony z folderu lokalnego.

Zdalna instalacja aplikacji na urządzeniach z zainstalowanym Agentem sieciowym

Jeśli na urządzeniu jest zainstalowany działający Agent sieciowy, połączony z głównym Serwerem administracyjnym (lub jednym z jego Serwerów podrzędnych), możesz zaktualizować Agenta sieciowego na tym urządzeniu, a także zainstalować, zaktualizować lub usunąć dowolne obsługiwane aplikacje poprzez Agenta sieciowego.

Możesz włączyć tę opcję, zaznaczając pole **Przy użyciu Agenta sieciowego** we właściwościach zadania zdalnej instalacji.

Jeśli to pole jest zaznaczone, pakiety instalacyjne z ustawieniami instalacji, zdefiniowanymi przez administratora, zostaną przesłane na urządzenia docelowe poprzez kanały komunikacyjne między Agentem sieciowym a Serwerem administracyjnym.

Aby zoptymalizować obciążenie na Serwerze administracyjnym oraz zminimalizować ruch pomiędzy Serwerem administracyjnym a urządzeniami, należy wskazać punkty dystrybucji w każdej sieci zdalnej lub domenie rozgłoszeniowej (sekcja Informacje o punktach dystrybucji oraz sekcja Tworzenie struktury grup administracyjnych i przydzielanie punktów dystrybucji). W tym przypadku pakiety instalacyjne oraz ustawienia instalatora są rozsyłane z Serwera administracyjnego na urządzenia docelowe poprzez punkty dystrybucji.

Co więcej, możliwe jest użycie punktów dystrybucji do transmisyjnego (multiemisja) dostarczania pakietów instalacyjnych, co pozwala znacząco zmniejszyć ruch sieciowy podczas zdalnej instalacji aplikacji.

Podczas wysyłania pakietów instalacyjnych na urządzenia docelowe poprzez kanały komunikacyjne między Agentami sieciowymi a Serwerem administracyjnym, wszystkie pakiety instalacyjne, które zostały przygotowane do wysłania, zostaną także zbuforowane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Jeśli używanych jest kilka dużych pakietów instalacyjnych różnych typów oraz wykorzystywana jest duża liczba punktów dystrybucji, rozmiar tego folderu może drastycznie się powiększyć.

Nie można ręcznie usunąć plików z folderu FTServer. Jeśli oryginalne pakiety instalacyjne zostaną usunięte, odpowiednie dane zostaną automatycznie usunięte z folderu FTServer.

Wszystkie dane otrzymane po stronie punktów dystrybucji są zapisywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Nie można ręcznie usunąć plików z folderu $FTCITmp. Po zakończeniu działania zadań korzystających z danych z tego folderu, jego zawartość zostanie automatycznie usunięta.

Ponieważ pakiety instalacyjne są rozsyłane poprzez kanały komunikacyjne między Serwerem administracyjnym a Agentami sieciowymi z repozytorium pośredniczącego w formacie zoptymalizowanym dla transferów sieciowych, nie można wprowadzać żadnych zmian w pakietach instalacyjnych, przechowywanych w oryginalnym folderze każdego pakietu instalacyjnego. Takie zmiany nie zostałyby automatycznie zarejestrowane przez Serwer administracyjny. Jeśli chcesz ręcznie zmodyfikować pliki pakietów instalacyjnych (chociaż zalecane jest unikanie takiego rozwiązania), należy zmodyfikować dowolne ustawienia pakietu instalacyjnego w Konsoli administracyjnej. Zmodyfikowanie ustawień pakietu instalacyjnego w Konsoli administracyjnej spowoduje, że Serwer administracyjny zaktualizuje obraz pakietu w pamięci podręcznej, który został przygotowany do przesłania na urządzenia docelowe.

Zarządzanie ponownym uruchamianiem urządzeń w zadaniu zdalnej instalacji

Aby zakończyć zdalną instalację aplikacji, często wymagane jest ponowne uruchomienie urządzeń (szczególnie w systemie Windows).

Jeśli korzystasz z zadania zdalnej instalacji z Kaspersky Security Center, w Kreatorze tworzenia nowego zadania lub w oknie właściwości zadania, które zostało utworzone (**sekcja Ponowne uruchomienie systemu operacyjnego**), możesz wybrać akcję, która zostanie wykonana, gdy wymagane będzie ponowne uruchomienie:

- **Nie uruchamiaj ponownie urządzenia**. W tym przypadku komputer nie zostanie automatycznie uruchomiony ponownie. Aby zakończyć instalację, należy uruchomić urządzenie ponownie (na przykład ręcznie lub przy użyciu zadania zarządzania urządzeniem). Informacje o wymaganym ponownym uruchomieniu zostaną zapisane w wynikach zadania oraz w statusie urządzenia. Opcja ta jest odpowiednia dla zadań instalacji na serwerach i innych urządzeniach, na których działanie ciągłe jest krytyczne.

- **Uruchom urządzenie ponownie**. W tym przypadku urządzenie jest zawsze automatycznie uruchamiane ponownie, jeśli jest to wymagane do zakończenia instalacji. Opcja jest przydatna, gdy zadania instalacji są uruchamiane na urządzeniach, na których możliwe są regularne przerwy w działaniu (wyłączenie lub ponowne uruchomienie).

- **Pytaj użytkownika o akcję**. W tym przypadku, na urządzeniu klienckim wyświetlane jest przypomnienie o ręcznym ponownym uruchomieniu urządzenia. Dla tej opcji można zdefiniować pewne ustawienia zaawansowane: treść wyświetlanego komunikatu, częstotliwość wyświetlania wiadomości oraz przedział czasu, po upływie którego ponowne uruchomienie zostanie wymuszone (bez potwierdzenia ze strony użytkownika). Opcja **Pytaj użytkownika o akcję** jest najodpowiedniejsza dla stacji roboczych, na których użytkownicy muszą mieć możliwość wyboru odpowiedniej godziny ponownego uruchomienia komputera.

Aktualizowanie baz danych w pakiecie instalacyjnym aplikacji antywirusowej

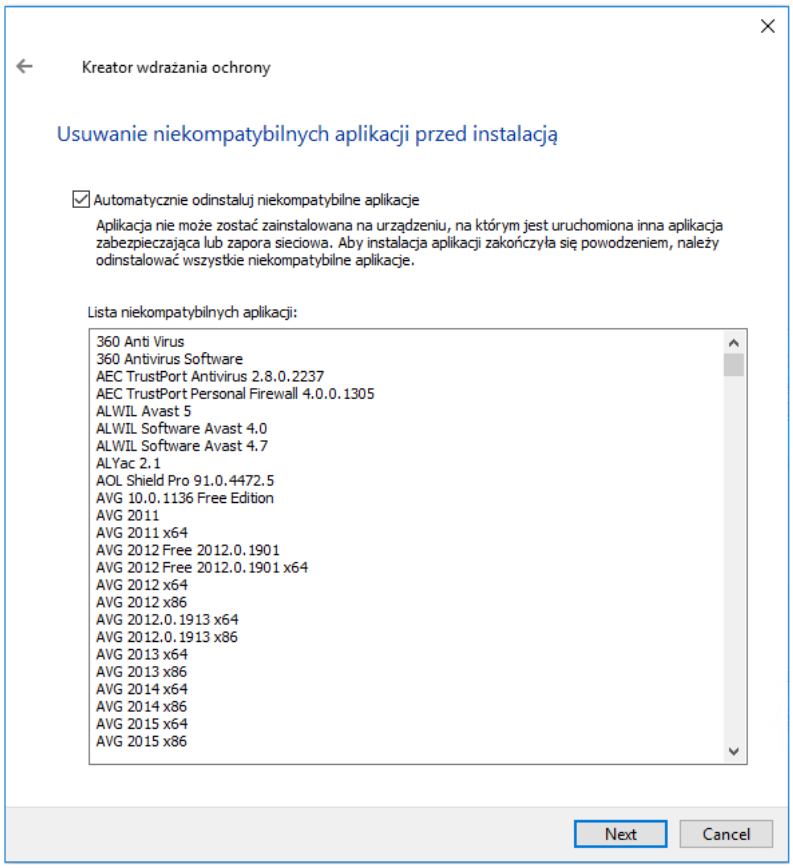
Przed rozpoczęciem wdrażania ochrony należy pamiętać o możliwości aktualizacji antywirusowych baz danych (w tym modułów i łat), dostarczanych wraz z pakietem dystrybucyjnym aplikacji zabezpieczającej. Dobrym rozwiązaniem jest zaktualizowanie baz danych w pakiecie instalacyjnym aplikacji przed rozpoczęciem wdrożenia (na przykład przy użyciu odpowiedniego polecenia z menu kontekstowego wybranego pakietu instalacyjnego). Zmniejszy to liczbę ponownych uruchomień wymaganych do zakończenia wdrożenia ochrony na urządzeniach docelowych. Jeśli zdalna instalacja wykorzystuje pakiety instalacyjne, które zostały przekazane do Serwerów wirtualnych z głównego Serwera administracyjnego, należy tylko zaktualizować bazy danych w oryginalnym pakiecie na Serwerze głównym. W tym przypadku nie ma konieczności aktualizowania baz danych w przekazanych pakietach na Serwerach wirtualnych.

Usuwanie niekompatybilnych aplikacji zabezpieczających firm trzecich

Instalacja aplikacji zabezpieczających firmy Kaspersky poprzez Kaspersky Security Center może wymagać usunięcia oprogramowania firmy trzeciej niekompatybilnego z instalowaną aplikacją. Istnieją dwa sposoby odinstalowania aplikacji innych firm.

Automatyczne usuwanie niekompatybilnych aplikacji przy użyciu instalatora

Po uruchomieniu instalatora wyświetla listę aplikacji, które nie są kompatybilne z aplikacją firmy Kaspersky:



Lista niekompatybilnych aplikacji wyświetlana w Kreatorze zdalnej instalacji

Kaspersky Security Center wykrywa niekompatybilne oprogramowanie. W związku z tym możesz zaznaczyć pole wyboru **Automatycznie odinstaluj niekompatybilne aplikacje**, aby kontynuować instalację. Jeśli usuniesz to pole wyboru i nie odinstalujesz niekompatybilnego oprogramowania, wystąpi błąd i aplikacja Kaspersky nie zostanie zainstalowana.

Automatyczne usuwanie niekompatybilnych aplikacji jest obsługiwane przez różne typy instalacji.

Dezinstalowanie niekompatybilnych aplikacji przy użyciu dedykowanego zadania

Aby usunąć niekompatybilne aplikacje, użyj zadania *Zdalna dezinstalacja aplikacji* Zadanie to powinno być uruchomione przed zadaniem instalacji aplikacji zabezpieczającej. Na przykład, w zadaniu instalacji możesz wybrać opcję terminarza **Po zakończeniu wykonywania innego zadania**, gdzie inne zadanie to *Zdalna dezinstalacja aplikacji*

Ta metoda dezinstalacji jest przydatna, jeśli instalator aplikacji zabezpieczającej nie może skutecznie usunąć niekompatybilnej aplikacji.

Korzystanie z narzędzi do zdalnej instalacji aplikacji z Kaspersky Security Center do uruchamiania odpowiednich plików wykonywalnych na zarządzanych urządzeniach

Korzystając z Kreatora tworzenia nowego pakietu, możesz wybrać dowolny plik wykonywalny i zdefiniować dla niego ustawienia wiersza poleceń. W tym celu należy dodać do pakietu instalacyjnego sam wybrany plik lub cały folder, w którym ten plik się znajduje. Następnie konieczne jest utworzenie zadania zdalnej instalacji i wybranie utworzonego pakietu instalacyjnego.

Podczas wykonywania zadania, na urządzeniach docelowych zostanie uruchomiony określony plik wykonywalny ze zdefiniowanymi ustawieniami wiersza poleceń.

Jeśli używasz instalatorów w formacie Microsoft Windows Installer (MSI), Kaspersky Security Center przeanalizuje wyniki instalacji przy użyciu standardowych narzędzi.

Jeśli dostępna jest licencja Zarządzania lukami i poprawkami, Kaspersky Security Center (podczas tworzenia pakietu instalacyjnego dla dowolnej obsługiwanej aplikacji w środowisku korporacyjnym) użyje także reguł do zainstalowania i przeanalizowania wyników instalacji, które znajdują się w jego aktualizowanej bazie danych.

W innym przypadku domyślne zadanie dla plików wykonywalnych poczeka na zakończenie uruchomionych procesów i wszystkich jego procesów podrzędnych. Po zakończeniu wszystkich uruchomionych procesów, zadanie zostanie zakończone pomyślnie niezależnie od kodu zwrotnego procesu instalacji. Aby zmienić takie zachowanie tego zadania, przed utworzeniem zadania należy ręcznie zmodyfikować pliki .kpd, które zostały wygenerowane przez Kaspersky Security Center w folderze nowo utworzonego pakietu instalacyjnego i jego podfolderach.

Aby zadanie nie czekało na zakończenie uruchomionych procesów, w sekcji [SetupProcessResult] ustaw wartość ustawienia Wait na 0:

Na przykład:
```
[SetupProcessResult]
Wait=0
```

Aby zadanie czekało tylko na zakończenie uruchomionych procesów w systemie Windows, a nie na zakończenie procesów podrzędnych, w sekcji [SetupProcessResult] ustaw wartość ustawienia WaitJob na 0, na przykład:

Na przykład:
```
[SetupProcessResult]
WaitJob=0
```

Aby zadanie zakończyło się pomyślnie lub zwróciło kod błędu w zależności od kodu zwrotnego uruchomionego procesu, w sekcji [SetupProcessResult_SuccessCodes] umieść listę pomyślnych kodów zwrotnych, na przykład:

Na przykład:
```
[SetupProcessResult_SuccessCodes]
0=
3010=
```

W tym przypadku każdy kod inny niż te znajdujące się na liście będzie zwracany jako błąd.

W celu wyświetlenia wiersza z komentarzem na temat pomyślnego zakończenia zadania lub błędu w wynikach zadania, w sekcji [SetupProcessResult_SuccessCodes] i [SetupProcessResult_ErrorCodes] wpisz krótki opis błędów odpowiadających kodom zwrotnym procesu, na przykład:

Na przykład:

[SetupProcessResult_SuccessCodes]

0= Instalacja zakończona pomyślnie

3010=Do zakończenia instalacji wymagane jest ponowne uruchomienie

[SetupProcessResult_ErrorCodes]

1602=Instalacja anulowana przez użytkownika

1603=Fatalny błąd podczas instalacji

W celu użycia narzędzi Kaspersky Security Center do zarządzania ponownym uruchomieniem urządzenia (jeśli ponowne uruchomienie jest wymagane do zakończenia działania), w sekcji [SetupProcessResult_NeedReboot] umieść listę kodów zwrotnych procesu, które wskazują na konieczność ponownego uruchomienia komputera:

Na przykład:

[SetupProcessResult_NeedReboot]

3010=

Monitorowanie zdalnej instalacji

W celu monitorowania instalacji Kaspersky Security Center oraz upewnienia się, że aplikacja zabezpieczająca i Agent sieciowy są zainstalowane na zarządzanych urządzeniach należy sprawdzić wskaźnik w sekcji **Wdrażanie**. Wskaźnik ten zlokalizowany jest w obszarze roboczym węzła Serwera administracyjnego w oknie głównym Konsoli administracyjnej. Kolory wskaźnika odzwierciedlają bieżący stan zdalnej instalacji. Obok wskaźnika wyświetlana jest liczba urządzeń, na których jest zainstalowany Agent sieciowy i aplikacje zabezpieczające. Jeśli uruchomione są jakiekolwiek zadania instalacji, postęp ich wykonania możesz monitorować w tym miejscu. Jeśli wystąpią jakiekolwiek błędy instalacyjne, liczba błędów zostanie wyświetlona w tym miejscu. Szczegóły dotyczące błędów można wyświetlić, klikając odnośnik.

Możesz także wykorzystać schemat zdalnej instalacji z obszaru roboczego folderu **Zarządzane urządzenia** na zakładce **Grupy**. Wykres odzwierciedla proces zdalnej instalacji i wyświetla liczbę urządzeń bez Agenta sieciowego, z Agentem sieciowym lub z Agentem sieciowym i aplikacją zabezpieczającą.

Więcej informacji o postępie wykonania zdalnej instalacji (lub działaniu określonego zadania instalacji) można uzyskać, otwierając okno wyników odpowiedniego zadania zdalnej instalacji: Kliknij zadanie prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Wyniki**. Okno będzie wyświetlało dwie listy: górna lista zawiera stany zadania na urządzeniach, natomiast dolna lista zawiera zdarzenia zadania na urządzeniu, które jest aktualnie wybrane na górnej liście.

Informacje o błędach zdalnej instalacji zostaną dodane do dziennika zdarzeń aplikacji Kaspersky na Serwerze administracyjnym. Informacje o błędach są także dostępne w odpowiednim wyborze zdarzeń, w folderze **Raporty i powiadomienia**, w podfolderze **Zdarzenia**.

Konfigurowanie instalatorów

Ta sekcja zawiera informacje na temat plików instalatorów Kaspersky Security Center i ustawień instalacji, a także zalecenia dotyczące instalacji Serwera administracyjnego i Agenta sieciowego w trybie cichym.

Informacje ogólne

Instalatory komponentów Kaspersky Security Center 14.2 (Serwer administracyjny, Agent sieciowy i Konsola administracyjna) bazują na technologii Instalatora Windows. Pakiet MSI jest podstawą instalatora. Ten format pakietów umożliwia wykorzystanie wszystkich korzyści oferowanych przez Instalator Windows: skalowalność, dostępność systemu poprawek, system transformacji, scentralizowana instalacja za pośrednictwem rozwiązań firm trzecich oraz niewidoczna rejestracja w systemie operacyjnym.

Instalacja w trybie cichym (z plikiem odpowiedzi)

Instalatory Serwera administracyjnego i Agenta sieciowego mogą pracować z plikiem odpowiedzi (ss_install.xml), w którym zintegrowane są parametry instalacji w trybie cichym bez udziału użytkownika. Plik ss_install.xml znajduje się w tym samym folderze co pakiet MSI. Jest on używany automatycznie podczas instalacji w trybie cichym. Możesz włączyć tryb cichej instalacji z użyciem przełącznika „/s" wiersza polecenia.

Na przykład:

```
setup.exe /s
```

Przed uruchomieniem instalatora w trybie cichym przeczytaj Umowę licencyjną użytkownika końcowego (EULA). Jeśli pakiet dystrybucyjny Kaspersky Security Center nie zawiera pliku TXT z treścią umowy EULA, możesz pobrać ten plik ze strony internetowej Kaspersky.

Plik ss_install.xml jest wewnętrznym formatem parametrów instalatora Kaspersky Security Center. Pakiety dystrybucyjne zawierają plik ss_install.xml z domyślnymi parametrami.

Nie należy ręcznie modyfikować pliku ss_install.xml. Ten plik może być modyfikowany tylko przy użyciu narzędzi Kaspersky Security Center podczas edytowania parametrów pakietów instalacyjnych w Konsoli administracyjnej.

W celu zmodyfikowania pliku odpowiedzi dla instalacji Serwera administracyjnego:

1. Otwórz pakiet dystrybucyjny Kaspersky Security Center. Jeśli używasz pełnego pakietu pliku EXE, rozpakuj go.
2. Utwórz folder Serwer, otwórz wiersz polecenia, a następnie uruchom następujące polecenie:
   ```
   setup.exe /r ss_install.xml
   ```
   Plik instalacyjny Kaspersky Security Center uruchomi się.
3. Postępuj zgodnie z instrukcjami kreatora, aby skonfigurować instalację Kaspersky Security Center.

   Po zakończeniu działania kreatora plik odpowiedzi jest automatycznie modyfikowany zgodnie z nowymi ustawieniami określonymi przez użytkownika.

Instalacja Agenta sieciowego w trybie cichym (bez pliku odpowiedzi)

Agenta sieciowego można zainstalować przy użyciu jednego pakietu .msi, określając wartości właściwości MSI w standardowy sposób. Ten scenariusz umożliwia zainstalowanie Agenta sieciowego przy użyciu profili grupy. Aby uniknąć konfliktów pomiędzy parametrami zdefiniowanymi poprzez właściwości MSI a parametrami zdefiniowanymi w pliku odpowiedzi, możesz wyłączyć plik odpowiedzi, ustawiając właściwość `DONT_USE_ANSWER_FILE=1`. Poniżej znajduje się przykład uruchomienia instalatora Agenta sieciowego z pakietem .msi.

Instalacja Agenta sieciowego w trybie nieinteraktywnym wymaga akceptacji warunków Umowy licencyjnej. Użyj parametru `EULA=1` tylko wtedy, gdy w pełni przeczytałeś, zrozumiałeś i zaakceptowałeś warunki Umowy licencyjnej.

Na przykład:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Możliwe jest także zdefiniowanie parametrów instalacji dla pakietu .msi poprzez wcześniejsze przygotowanie pliku odpowiedzi (z rozszerzeniem .mst). To polecenie wygląda następująco:

Na przykład:

```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

W jednym poleceniu można określić kilka plików odpowiedzi.

Częściowa konfiguracja instalacji poprzez setup.exe

Podczas uruchamiania instalacji aplikacji z pliku setup.exe, do pakietu MSI możesz dodać wartości dowolnych właściwości MSI.

To polecenie wygląda następująco:

Na przykład:

```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parametry instalacji Serwera administracyjnego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Serwera administracyjnego. Wszystkie parametry są opcjonalne, za wyjątkiem EULA i PRIVACYPOLICY.

Parametry instalacji Serwera administracyjnego w trybie nieinteraktywnym

Właściwość MSI	Opis	Dostępne wartości
EULA	Akceptacja postanowień i warunków Umowy licencyjnej (wymagana)	• 1—W pełni przeczytałem, rozumiem i akceptuję warunki Umowy licencyjnej. • Inna wartość lub bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
PRIVACYPOLICY	Akceptacja postanowień i warunków Polityki prywatności (wymagana)	• 1—Jestem świadomy i wyrażam zgodę na przetwarzanie oraz przesyłanie moich danych (również do innych krajów) zgodnie z Polityką prywatności. Potwierdzam, że w pełni przeczytałem i rozumiem Politykę prywatności. • Inna wartość lub bez wartości—Nie akceptuję postanowień i warunków

		Polityki prywatności (instalacja nie zostanie wykonana).
INSTALLATIONMODETYPE	Typ instalacji Serwera administracyjnego	• Standardowa. • Niestandardowa.
INSTALLDIR	Folder instalacyjny aplikacji	Wartość wiersza.
ADDLOCAL	Lista komponentów przeznaczonych do zainstalowania (oddzielone przecinkami)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Minimalna lista komponentów wystarczających do poprawnego zainstalowania Serwera administracyjnego: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Rozmiar sieci	• NRT_1_100 — od 1 do 100 urządzeń. • NRT_100_1000 – od 101 do 1 000 urządzeń. • NRT_GREATER_1000—więcej niż 1 000 urządzeń. Ten parametr potwierdza, że w pełni przeczytałeś, zrozumiałeś i zaakceptowałeś warunki Umowy licencyjnej.
SRV_ACCOUNT_TYPE	Sposób określania użytkownika dla działania usługi Serwera administracyjnego	• SrvAccountDefault—konto użytkownika zostanie utworzone automatycznie • SrvAccountUser—konto użytkownika jest określane ręcznie.
SERVERACCOUNTNAME	Nazwa użytkownika dla usługi	Wartość wiersza.
SERVERACCOUNTPWD	Hasło użytkownika dla usługi	Wartość wiersza.
DBTYPE	Typ bazy danych	• MySQL—używana będzie baza danych MySQL lub MariaDB. • MSSQL—używana będzie baza danych Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	Pełna nazwa serwera MySQL lub MariaDB	Wartość wiersza.
MYSQLSERVERPORT	Numer portu używanego do nawiązania połączenia z	Wartość numeryczna.

	serwerem MySQL lub MariaDB	
MYSQLDBNAME	Nazwa bazy danych serwera MySQL lub Maria DB	Wartość wiersza.
MYSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z bazą danych serwera MySQL lub MariaDB	Wartość wiersza.
MYSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z bazą danych serwera MySQL lub MariaDB	Wartość wiersza.
MSSQLCONNECTIONTYPE	Sposób użycia bazy danych MSSQL	• InstallMSSEE—instalacja z pakietu • ChooseExisting—użycie zainstalowanego serwera.
MSSQLSERVERNAME	Pełna nazwa instancji serwera SQL	Wartość wiersza.
MSSQLDBNAME	Nazwa bazy danych serwera SQL	Wartość wiersza.
MSSQLAUTHTYPE	Metoda autoryzacji podczas nawiązywania połączenia z serwerem SQL	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nazwa użytkownika nawiązującego połączenie z serwerem SQL w trybie SQLServer	Wartość wiersza.
MSSQLACCOUNTPWD	Hasło użytkownika nawiązującego połączenie z serwerem SQL w trybie SQLServer	Wartość wiersza.

CREATE_SHARE_TYPE	Metoda określania folderu współdzielonego	• Create—tworzy nowy folder współdzielony. W takim przypadku należy zdefiniować następujące właściwości:
		  • SHARELOCALPATH—ścieżka dostępu do folderu lokalnego.
		  • SHAREFOLDERNAME—nazwa sieciowa folderu.
		• Null—należy określić właściwość EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Pełna ścieżka dostępu do istniejącego folderu współdzielonego	Wartość wiersza.
SERVERPORT	Numer portu używanego do	Wartość numeryczna.

	nawiązania połączenia z Serwerem administracyjnym	
SERVERSSLPORT	Numer portu używanego do nawiązania bezpiecznego połączenia SSL z Serwerem administracyjnym	Wartość numeryczna.
SERVERADDRESS	Adres Serwera administracyjnego	Wartość wiersza.
SERVERCERT2048BITS	Długość klucza certyfikatu Serwera administracyjnego (bity)	• 1—długość klucza certyfikatu Serwera administracyjnego wynosi 2048 bity. • 0 — długość klucza certyfikatu Serwera administracyjnego wynosi 1024 bity. • Jeśli nie określono wartości, długość klucza certyfikatu Serwera administracyjnego wynosi 1024 bity.
MOBILESERVERADDRESS	Adres Serwera administracyjnego do nawiązywania połączenia z urządzeniami mobilnymi; ignorowane, jeśli nie wybrano komponentu MobileSupport	Wartość wiersza.

Parametry instalacji Agenta sieciowego

Poniższa tabela opisuje właściwości MSI, które można skonfigurować podczas instalacji Agenta sieciowego. Wszystkie parametry są opcjonalne, za wyjątkiem EULA i SERVERADDRESS.

Parametry instalacji Agenta sieciowego w trybie nieinteraktywnym

Właściwość MSI	Opis	Dostępne wartości
EULA	Akceptacja postanowień i warunków Umowy licencyjnej	• 1—W pełni przeczytałem, rozumiem i akceptuję warunki Umowy licencyjnej. • 0—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana). • Bez wartości—Nie akceptuję postanowień i warunków Umowy licencyjnej (instalacja nie zostanie wykonana).
DONT_USE_ANSWER_FILE	Odczyt ustawień instalacji z pliku odpowiedzi	• 1—Nie używaj.

		• Inna wartość lub brak wartości—Odczyt.
INSTALLDIR	Ścieżka do folderu instalacyjnego Agenta sieciowego	Wartość wiersza.
SERVERADDRESS	Adres Serwera administracyjnego (wymagane)	Wartość wiersza.
SERVERPORT	Numer portu używanego do nawiązania połączenia z Serwerem administracyjnym	Wartość numeryczna.
SERVERSSLPORT	Numer portu dla szyfrowanego połączenia z Serwerem administracyjnym przy użyciu protokołu SSL	Wartość numeryczna.
USESSL	Czy użyć połączenia SSL	• 1—użyj. • Inna wartość lub brak wartości—nie używaj.
OPENUDPPORT	Czy otworzyć port UDP	• 1—otwórz. • Inna wartość lub brak wartości—nie otwieraj.
UDPPORT	Numer portu UDP	Wartość numeryczna.
USEPROXY	Czy użyć serwera proxy	• 1—użyj. • Inna wartość lub brak wartości—nie używaj.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Adres proxy i numer portu używanego do nawiązania połączenia z serwerem proxy	Wartość wiersza.
PROXYLOGIN	Konto używane do nawiązywania połączenia z serwerem proxy	Wartość wiersza.
PROXYPASSWORD	Hasło do konta dla połączenia z serwerem proxy (W parametrach pakietów instalacyjnych nie należy określać żadnych szczegółów kont użytkowników uprzywilejowanych.)	Wartość wiersza.
GATEWAYMODE	Tryb użycia bramy połączenia	• 0—nie używaj bramy połączenia. • 1—użyj tego Agenta sieciowego jako bramy połączenia. • 2—połącz z Serwerem administracyjnym przy użyciu bramy połączenia.

GATEWAYADDRESS	Adres bramy połączenia	Wartość wiersza.
CERTSELECTION	Metoda pobierania certyfikatu	• GetOnFirstConnection—uzyskaj certyfikat z Serwera administracyjnego. • GetExistent—wybierz istniejący certyfikat. Jeśli ta opcja zostanie wybrana, należy określić właściwość CERTFILE.
CERTFILE	Ścieżka do pliku certyfikatu	Wartość wiersza.
VMVDI	Włącz tryb dynamiczny dla wirtualnej infrastruktury pulpitu Virtual Desktop Infrastructure (VDI).	• 1—włącz. • 0—nie włączaj. • Brak wartości—nie włączaj.
LAUNCHPROGRAM	Czy uruchomić usługę Agenta sieciowego po instalacji	• 1—uruchom. • Inna wartość lub brak wartości—nie uruchamiaj.
NAGENTTAGS	Znacznik dla Agenta sieciowego (ma priorytet nad znacznikiem podanym w pliku odpowiedzi)	Wartość wiersza.

Infrastruktura wirtualna

Kaspersky Security Center obsługuje użycie maszyn wirtualnych. Możesz zainstalować Agenta sieciowego i aplikację zabezpieczającą na każdej maszynie wirtualnej, a także wdrożyć ochronę maszyn wirtualnych na poziomie hipernadzorcy. W pierwszym przypadku, do ochrony maszyn wirtualnych możesz użyć standardowej aplikacji zabezpieczającej lub Kaspersky Security for Virtualization Light Agent. W drugim przypadku możesz użyć Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center obsługuje przywracanie maszyn wirtualnych do ich poprzedniego stanu.

Wskazówki dotyczące zmniejszenia obciążenia na maszynach wirtualnych

Podczas instalacji Agenta sieciowego na maszynie wirtualnej zalecane jest rozważenie wyłączenia funkcji Kaspersky Security Center, które nie będą zbyt przydatne dla maszyn wirtualnych.

Podczas instalacji Agenta sieciowego na maszynie wirtualnej lub na szablonie przeznaczonym do wygenerowania maszyn wirtualnych, zalecane jest wykonanie następujących czynności:

- Jeśli uruchamiasz zdalną instalację, w oknie właściwości pakietu instalacyjnego Agenta sieciowego, w sekcji **Zaawansowane** zaznacz opcję **Optymalizuj ustawienia dla VDI**.
- Jeśli uruchamiasz instalację w trybie interaktywnym z udziałem kreatora, w oknie kreatora zaznacz opcję **Optymalizuj ustawienia Agenta sieciowego dla infrastruktury wirtualnej**.

Zaznaczenie tych opcji spowoduje zmianę ustawień Agenta sieciowego w taki sposób, że poniższe funkcje pozostaną domyślnie wyłączone (przed zastosowaniem zasady):

- Zbieranie informacji o zainstalowanym oprogramowaniu
- Zbieranie informacji o sprzęcie
- Zbieranie informacji o wykrytych lukach
- Zbieranie informacji o wymaganych aktualizacjach

Zazwyczaj te funkcje nie są potrzebne na maszynach wirtualnych, gdyż wykorzystują stałe oprogramowanie i sprzęt wirtualny.

Wyłączenie tych funkcji jest odwracalne. Jeśli jakakolwiek z wyłączonych funkcji jest potrzebna, możesz ją włączyć poprzez profil Agenta sieciowego lub poprzez ustawienia lokalne Agenta sieciowego. Ustawienia lokalne Agenta sieciowego są dostępne poprzez menu kontekstowe odpowiedniego urządzenia w Konsoli administracyjnej.

Obsługa dynamicznych maszyn wirtualnych

Kaspersky Security Center obsługuje dynamiczne maszyny wirtualne. Jeśli w sieci organizacji została wdrożona infrastruktura wirtualna, w pewnych przypadkach możliwe będzie korzystanie z dynamicznych (tymczasowych) maszyn wirtualnych. Dynamiczne maszyny wirtualne są tworzone pod unikatowymi nazwami w oparciu o szablony, które zostały przygotowane przez administratora. Użytkownik pracuje na maszynie wirtualnej przez jakiś czas, a następnie, po wyłączeniu maszyny zostanie ona usunięta z infrastruktury wirtualnej. Jeśli w sieci organizacji jest zainstalowany program Kaspersky Security Center, maszyna wirtualna z zainstalowanym Agentem sieciowym zostanie dodana do bazy danych Serwera administracyjnego. Po wyłączeniu maszyny wirtualnej, odpowiedni wpis musi także zostać usunięty z bazy danych Serwera administracyjnego.

Aby funkcja automatycznego usuwania wpisów na temat maszyn wirtualnych mogła działać, podczas instalacji Agenta sieciowego na szablonie dla dynamicznych maszyn wirtualnych wybierz opcję **Włącz tryb dynamiczny VDI**:

- Dla zdalnej instalacji—w oknie właściwości pakietu instalacyjnego Agenta sieciowego (sekcja **Zaawansowane**)
- Dla instalacji w trybie interaktywnym—w Kreatorze instalacji Agenta sieciowego

> Staraj się unikać zaznaczania opcji **Włącz tryb dynamiczny VDI** podczas instalacji Agenta sieciowego na urządzeniach fizycznych.

Jeśli chcesz, żeby zdarzenia z dynamicznych maszyn wirtualnych były przechowywane na Serwerze administracyjnym przez jakiś czas po usunięciu tych maszyn wirtualnych, w oknie właściwości Serwera administracyjnego, w sekcji **Repozytorium zdarzeń** wybierz opcję **Przechowuj zdarzenia po usunięciu urządzeń** i określ maksymalny czas przechowywania zdarzeń (w dniach).

Obsługa kopiowania maszyn wirtualnych

Kopiowanie maszyn wirtualnych z zainstalowanym Agentem sieciowym lub tworzenie maszyny wirtualnej z szablonu z zainstalowanym Agentem sieciowym odbywa się w ten sam sposób co zdalna instalacja Agenta sieciowego poprzez przechwycenie i skopiowanie obrazu dysku twardego. Oznacza to, że podczas kopiowania maszyn wirtualnych należy wykonać te same czynności, co podczas instalacji Agenta sieciowego poprzez skopiowanie obrazu dysku.

Jednakże dwa poniższe przypadki przedstawiają sytuacje, gdy Agent sieciowy automatycznie wykrywa kopiowanie. Dzięki temu nie ma potrzeby wykonywania wszystkich skomplikowanych działań wymienionych w sekcji "Zdalna instalacja poprzez przechwycenie i skopiowanie obrazu dysku twardego urządzenia":

- Opcja **Włącz tryb dynamiczny VDI** została wybrana po zainstalowaniu Agenta sieciowego - po każdym ponownym uruchomieniu systemu operacyjnego ta maszyna wirtualna będzie rozpoznawana jako nowe urządzenie, niezależnie od tego, czy została skopiowana.

- Używany jest jeden z następujących hipernadzorców: VMware™, HyperV® lub Xen®: Agent sieciowy wykrywa kopiowanie maszyny wirtualnej po zmienionych numerach ID sprzętu wirtualnego.

Analiza zmian w sprzęcie wirtualnym nie jest całkowicie wiarygodna. Przed szerszym zastosowaniem tej metody należy ją sprawdzić na małej puli maszyn wirtualnych dla wersji hipernadzorcy, który jest aktualnie używany w organizacji.

Obsługa przywracania systemu plików dla urządzeń z zainstalowanym Agentem sieciowym

Kaspersky Security Center jest aplikacją oferującą wiele funkcji. Przywrócenie poprzedniego stanu systemu plików na urządzeniu z zainstalowanym Agentem sieciowym doprowadzi do desynchronizacji danych i niepoprawnego działania Kaspersky Security Center.

Wycofanie systemu plików (lub jego części) może zostać wykonane w następujących przypadkach:

- Podczas kopiowania obrazu dysku twardego.

- Podczas przywracania stanu maszyny wirtualnej przy użyciu infrastruktury wirtualnej.

- Podczas przywracania danych z kopii zapasowej lub punktu odzyskiwania.

Scenariusze, w których oprogramowanie firm trzecich na urządzeniach z zainstalowanym Agentem sieciowym wpływa na zawartość folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\, są dla Kaspersky Security Center tylko krytycznymi scenariuszami. Dlatego też, jeśli to tylko możliwe, powinieneś zawsze wykluczać ten folder z procedury odzyskiwania.

Ponieważ zasady działania niektórych organizacji dopuszczają możliwość wycofania systemu plików urządzeń, obsługa wycofania systemu plików na urządzeniach z zainstalowanym Agentem sieciowym jest dostępna w Kaspersky Security Center od wersji 10 Maintenance Release 1 (Serwer administracyjny i Agenty sieciowe muszą być w wersjach 10 Maintenance Release 1 lub nowszych). Po wykryciu takich urządzeń są one automatycznie ponownie łączone z Serwerem administracyjnym z całkowitym wyczyszczeniem danych i pełną synchronizacją.

Domyślnie obsługa wykrywania wycofania systemu plików jest włączona w Kaspersky Security Center 14.2.

Jeśli jest to tylko możliwe, unikaj przywracania poprzedniego stanu folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ na urządzeniach z zainstalowanym Agentem sieciowym, gdyż całkowita ponowna synchronizacja danych zużywa dużą ilość zasobów.

Wycofanie stanu systemu jest całkowicie zabronione na urządzeniu z zainstalowanym Serwerem administracyjnym. Podobnie jest w przypadku wycofania baz danych używanych przez Serwer administracyjny.

Możesz przywrócić stan Serwera administracyjnego z kopii zapasowej tylko przy użyciu standardowego narzędzia klbackup.

Informacje o profilach połączenia dla użytkowników mobilnych

Mobilni użytkownicy laptopów (zwanych dalej również "urządzeniami") mogą potrzebować zmiany metody łączenia się z Serwerem administracyjnym lub przełączania pomiędzy Serwerami administracyjnymi w zależności od aktualnej lokalizacji urządzenia w sieci firmowej.

Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows i macOS.

Używanie różnych adresów jednego Serwera administracyjnego

Urządzenia z zainstalowanym Agentem sieciowym mogą łączyć się z Serwerem administracyjnym z poziomu wewnętrznej sieci organizacji lub Internetu. W tej sytuacji wymagane może być, aby Agent sieciowy używał innych adresów do łączenia się z Serwerem administracyjnym: zewnętrznego adresu Serwera administracyjnego dla połączenia internetowego oraz wewnętrznego adresu Serwera administracyjnego dla wewnętrznego połączenia sieciowego.

W tym celu musisz dodać profil (dla połączenia z Serwerem administracyjnym z poziomu internetu) do zasady Agenta sieciowego. Dodaj profil we właściwościach zasady (sekcja **Łączność**, podsekcja **Profile połączenia**). W oknie tworzenia profilu należy wyłączyć opcję **Użyj tylko do pobierania uaktualnień** oraz wybrać opcję **Synchronizuj ustawienia połączenia z ustawieniami Serwera administracyjnego określonymi w tym profilu**. Jeśli do łączenia się z Serwerem administracyjnym używasz bramy połączenia (na przykład, w konfiguracji Kaspersky Security Center, opisanej w sekcji Dostęp do internetu: Agent sieciowy jako brama połączenia w strefie zdemilitaryzowanej), w odpowiednim polu profilu połączenia musisz określić adres bramy połączenia.

Przełączanie pomiędzy Serwerami administracyjnymi w zależności od aktualnej sieci

Jeśli organizacja posiada kilka biur z różnymi Serwerami administracyjnymi, a niektóre urządzenia z zainstalowanym Agentem sieciowym są przenoszone pomiędzy nimi, Agent sieciowy musi łączyć się z Serwerem administracyjnym sieci lokalnej w biurze, w którym znajduje się urządzenie.

W tej sytuacji konieczne jest utworzenie profilu dla połączenia z Serwerem administracyjnym we właściwościach zasady Agenta sieciowego dla każdego z biur, za wyjątkiem głównego biura, w którym znajduje się oryginalny macierzysty Serwer administracyjny. W profilach połączenia należy określić adresy Serwerów administracyjnych i włączyć lub wyłączyć opcję **Użyj tylko do pobierania uaktualnień**:

- Wybierz tę opcję, jeśli chcesz, aby Agent sieciowy zsynchronizował się z macierzystym Serwerem administracyjnym, a Serwer lokalny był używany tylko do pobierania uaktualnień.
- Wyłącz tę opcję, jeśli Agent sieciowy ma być całkowicie zarządzany przez lokalny Serwer administracyjny.

Następnie powinieneś ustalić warunki przełączania do nowo utworzonych profili: przynajmniej jeden warunek dla każdego z biur, za wyjątkiem głównego biura. Celem każdego warunku jest wykrycie elementów, które są specyficzne dla środowiska sieciowego w biurze. Jeśli warunek jest prawdziwy, odpowiedni profil zostaje aktywowany. Jeśli żaden z warunków nie jest prawdziwy, Agent sieciowy przełączy się do macierzystego Serwera administracyjnego.

Wdrażanie funkcji Zarządzanie urządzeniami mobilnymi

Ta sekcja zawiera informacje o wstępnej instalacji funkcji Zarządzanie urządzeniami mobilnymi.

Połączenie urządzeń KES z Serwerem administracyjnym

W zależności od metody używanej do łączenia urządzeń z Serwerem administracyjnym, dla Kaspersky Device Management for iOS istnieją dwa schematy zdalnej instalacji na urządzeniach KES:

- Schemat zdalnej instalacji z bezpośrednim połączeniem urządzeń z Serwerem administracyjnym
- Schemat zdalnej instalacji uwzględniający Forefront® Threat Management Gateway (TMG)

Bezpośrednie połączenie urządzeń z Serwerem administracyjnym

Urządzenia KES mogą łączyć się bezpośrednio z portem 13292 Serwera administracyjnego.

W zależności od metody używanej do autoryzacji, dla połączenia urządzeń KES z Serwerem administracyjnym możliwe są dwie opcje:

- Łączenie urządzeń z użyciem certyfikatu użytkownika
- Łączenie urządzeń bez użycia certyfikatu użytkownika

Łączenie urządzeń z użyciem certyfikatu użytkownika

Podczas łączenia urządzeń z użyciem certyfikatu użytkownika, to urządzenie jest kojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

W tym przypadku używane będzie dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne). Serwer administracyjny i urządzenie będą uwierzytelniani przy użyciu certyfikatów.

Łączenie urządzeń bez użycia certyfikatu użytkownika

Podczas łączenia urządzenia bez użycia certyfikatu użytkownika, to urządzenie nie jest kojarzone z żadnym kontem użytkownika na Serwerze administracyjnym. Jednakże, gdy urządzenie pobierze dowolny certyfikat, to urządzenie zostanie skojarzone z kontem użytkownika, do którego odpowiedni certyfikat został przypisany poprzez narzędzia Serwera administracyjnego.

Podczas łączenia tego urządzenia z Serwerem administracyjnym zostanie zastosowane jednokierunkowe uwierzytelnianie SSL, co oznacza, że tylko Serwer administracyjny będzie uwierzytelniony przy użyciu certyfikatu. Po pobraniu przez urządzenie certyfikatu użytkownika, typ autoryzacji zmieni się na dwukierunkowe uwierzytelnianie SSL (uwierzytelnianie obustronne).

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD)

Schemat łączenia urządzeń KES z Serwerem wykorzystujący delegowanie protokołu Kerberos (KCD) uwzględnia:

- Integrację z Microsoft Forefront TMG.
- Użycie delegowania protokołu Kerberos (zwane również KCD) do uwierzytelnia urządzeń mobilnych.
- Integrację z infrastrukturą kluczy publicznych (zwana również PKI) w celu zastosowania certyfikatów użytkownika.

Podczas korzystania z tego schematu połączenia należy pamiętać, że:

- Typem połączenia urządzeń KES z TMG ma być "dwukierunkowe uwierzytelnianie SSL", czyli urządzenie musi łączyć się z TMG poprzez swój własny certyfikat użytkownika. W tym celu należy zintegrować certyfikat użytkownika z pakietem instalacyjnym programu Kaspersky Endpoint Security for Android, który został zainstalowany na urządzeniu. Ten pakiet KES musi być utworzony przez Serwer administracyjny specjalnie dla tego urządzenia (użytkownika).
- Dla protokołu mobilnego powinieneś określić specjalny (niestandardowy) certyfikat zamiast domyślnego certyfikatu serwera:

  1. W oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat**.
  2. W otwartym oknie określ ten sam certyfikat, który został ustawiony na TMG, gdy punkt dostępu do protokołu mobilnego został opublikowany na Serwerze administracyjnym.

- Certyfikaty użytkownika dla urządzeń KES muszą być wystawione przez urząd certyfikacji (CA) domeny. Należy pamiętać, że jeśli domena zawiera kilka głównych urzędów certyfikacji, certyfikaty użytkownika muszą być wystawione przez urząd certyfikacji, który został ustawiony w publikacji na TMG.

  Możesz upewnić się, że certyfikat użytkownika jest zgodny z wyżej opisanymi wymaganiami przy użyciu jednej z następujących metod:

  - Określ specjalny certyfikat użytkownika w kreatorze Nowego pakietu oraz kreatorze instalacji Certyfikatu.
  - Zintegruj Serwer administracyjny z infrastrukturą kluczy publicznych domeny oraz zdefiniuj odpowiednie ustawienie w regułach wystawiania certyfikatów:

    1. W drzewie konsoli rozwiń folder **Zarządzanie urządzeniami mobilnymi**, z którego wybierz podfolder **Certyfikaty**.
    2. W obszarze roboczym folderu **Certyfikaty** kliknij przycisk **Konfiguruj reguły wydawania certyfikatów**, aby otworzyć okno **Reguły wydawania certyfikatu**.
    3. W sekcji **Integracja z PKI** skonfiguruj integrację z infrastrukturą kluczy publicznych.
    4. W sekcji **Wydawanie certyfikatów dla urządzeń mobilnych** określ źródło certyfikatów.

Poniżej znajduje się przykład konfiguracji delegowania protokołu Kerberos (KCD) z następującymi założeniami:

- Punkt dostępu do protokołu mobilnego na Serwerze administracyjnym jest ustawiony na porcie 13292.
- Nazwa urządzenia z TMG to tmg.mydom.local.
- Nazwa urządzenia z Serwerem administracyjnym to ksc.mydom.local.
- Nazwa zewnętrznej publikacji punktu dostępu do protokołu mobilnego to kes4mob.mydom.global.

Konto domeny dla Serwera administracyjnego

Należy utworzyć konto domeny (na przykład: KSCMobileSrvcUsr), z poziomu którego będzie uruchamiana usługa Serwera administracyjnego. Konto dla usługi Serwera administracyjnego można określić podczas instalacji Serwera administracyjnego lub poprzez narzędzie klsrvswch. Narzędzie klsrvswch znajduje się w folderze instalacyjnym Serwera administracyjnego.

Konto domeny musi zostać określone z następujących względów:

- Funkcja zarządzania urządzeniami KES jest integralną częścią Serwera administracyjnego.
- Aby zapewnić poprawne działanie delegowania protokołu Kerberos (KCD), strona odbierająca (czyli Serwer administracyjny) musi być uruchomiona z poziomu konta domeny.

Nazwa główna usługi dla http/kes4mob.mydom.local

W domenie, z poziomu konta KSCMobileSrvcUsr, dodaj SPN dla publikacji usługi protokołu mobilnego na porcie 13292 urządzenia z Serwerem administracyjnym. Dla urządzenia kes4mob.mydom.local z Serwerem administracyjnym będzie to wyglądało w następujący sposób:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Konfigurowanie właściwości domeny urządzenia z TMG (tmg.mydom.local)

Aby przeprowadzić ruch sieciowy, przełącz urządzenie z TMG (tmg.mydom.local) do usługi, która jest definiowana po SPN (http/kes4mob.mydom.local:13292).

W celu przełączenia urządzenia z TMG do usługi definiowanej po SPN (http/kes4mob.mydom.local:13292), administrator musi wykonać następujące działania:

1. W przystawce Microsoft Management Console o nazwie „Użytkownicy i komputery usługi Active Directory" wybierz urządzenie z zainstalowanym TMG (tmg.mydom.local).
2. We właściwościach urządzenia, na zakładce **Delegowanie** ustaw przełącznik **Ufaj temu komputerowi w delegowaniu tylko do określonych usług** na **Użyj dowolnego protokołu uwierzytelniania**.
3. Na liście **Usługi, którym to konto może przedstawiać delegowane poświadczenia** dodaj SPN http/kes4mob.mydom.local:13292.

Specjalny (niestandardowy) certyfikat dla publikacji (kes4mob.mydom.global)

Aby opublikować protokół mobilny Serwera administracyjnego, należy wystawić specjalny (niestandardowy) certyfikat dla FQDN kes4mob.mydom.global, a także określić go w miejsce domyślnego certyfikatu serwera w ustawieniach protokołu mobilnego Serwera administracyjnego, w Konsoli administracyjnej. W tym celu, w oknie właściwości Serwera administracyjnego, w sekcji **Ustawienia** zaznacz pole **Otwórz port dla urządzeń mobilnych**, a następnie z listy rozwijalnej wybierz **Dodaj certyfikat**.

Należy pamiętać, że kontener certyfikatów serwera (plik z rozszerzeniem .p12 lub .pfx) musi także zawierać łańcuch certyfikatów głównych (klucze publiczne).

Konfigurowanie publikacji na TMG

Na TMG, dla ruchu przechodzącego z urządzenia mobilnego do portu 13292 usługi kes4mob.mydom.global należy skonfigurować KCD na SPN (http/kes4mob.mydom.local:13292), korzystając z certyfikatu serwera opublikowanego dla FQDN kes4mob.mydom.global. Nie można zapominać, że publikacja oraz opublikowany punkt dostępu (port 13292 Serwera administracyjnego) powinny korzystać z tego samego certyfikatu serwera.

Korzystanie z Google Firebase Cloud Messaging

Aby zapewnić reakcję urządzeń KES z systemem Android w odpowiednim momencie na polecenia administratora, należy włączyć korzystanie z usługi Google™ Firebase Cloud Messaging (zwana również FCM) we właściwościach Serwera administracyjnego.

W celu włączenia korzystania z FCM:

1. W Konsoli administracyjnej wybierz węzeł **Zarządzanie urządzeniami mobilnymi** oraz folder **Urządzenia mobilne**.
2. Z otwartego menu kontekstowego folderu **Urządzenia mobilne** wybierz **Właściwości**.
3. We właściwościach folderu wybierz sekcję **Ustawienia Google Firebase Cloud Messaging**.
4. W polach **ID nadawcy** i **Klucz serwera** określ ustawienia FCM: ID_NADAWCY i Klucz API.

Usługa FCM działa w następujących zakresach adresów:

- Ze strony urządzenia KES dostęp jest wymagany do portów 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) oraz 5230 (HTTPS) dla następujących adresów:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169
- Ze strony Serwera administracyjnego dostęp jest wymagany do portu 443 (HTTPS) dla następujących adresów:
  - fcm.googleapis.com
  - Wszystkie adresy IP w ASN Google'a dla portu 15169

Jeśli ustawienia serwera proxy (**Zaawansowane** / **Konfiguracja dostępu do internetu**) zostały określone we właściwościach Serwera administracyjnego w Konsoli administracyjnej, będą używane do interakcji z FCM.

Konfigurowanie FCM: uzyskiwanie ID_NADAWCY i klucza API

W celu skonfigurowania FCM, administrator musi wykonać następujące akcje:

1. Zarejestrować się na portalu Google.
2. Przejść na portal deweloperów.
3. Utworzyć nowy projekt, klikając przycisk **Create Project**, określić nazwę projektu oraz ID.
4. Zaczekać, aż projekt zostanie utworzony.
   Na pierwszej stronie projektu, w górnej części strony pole **Project Number** wyświetli odpowiedni ID_NADAWCY.
5. Przejść do sekcji **APIs & auth / APIs** i włączyć **Google Firebase Cloud Messaging for Android**.
6. Przejść do sekcji **APIs & auth / Credentials** i kliknąć przycisk **Create New Key**.
7. Kliknij przycisk **Klucz serwera**.
8. Nałożyć ograniczenia (jeśli są) i kliknąć przycisk **Create**.
9. Uzyskać klucz API z właściwości nowo utworzonego klucza (pole **Klucz serwera**).

Integracja z infrastrukturą kluczy publicznych

Integracja z infrastrukturą kluczy publicznych (zwana również PKI) jest przeznaczona głównie do uproszenia wystawiania certyfikatów użytkownika domeny przez Serwer administracyjny.

Administrator może przypisać certyfikat domeny dla użytkownika w Konsoli administracyjnej. Można to zrobić przy użyciu jednej z następujących metod:

- Przydziel użytkownikowi specjalny (niestandardowy) certyfikat z pliku w kreatorze instalacji certyfikatu.
- Przeprowadź integrację z PKI i wskaż PKI jako źródło certyfikatów dla określonego typu certyfikatów lub dla wszystkich typów certyfikatów.

Ustawienia integracji z PKI są dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** po kliknięciu odnośnika **Zintegruj z infrastrukturą klucza publicznego**.

Ogólne zasady integracji z PKI dla publikacji certyfikatów użytkownika domeny

W Konsoli administracyjnej, w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** kliknij odnośnik **Zintegruj z infrastrukturą klucza publicznego**, aby określić konto domeny, które będzie używane przez Serwer administracyjny do wystawiania certyfikatów użytkownika domeny poprzez urząd certyfikacji domeny (zwany również kontem, z poziomu którego wykonywana jest integracja z PKI).

Należy pamiętać, że:

- Ustawienia integracji z PKI oferują możliwość określenia domyślnego szablonu dla wszystkich typów certyfikatów. Nie wolno też zapominać, że reguły wydawania certyfikatów (dostępne w obszarze roboczym folderu **Zarządzanie urządzeniami mobilnymi** / **Certyfikaty** po kliknięciu przycisku **Konfiguruj reguły wydawania certyfikatów**) pozwalają na określenie indywidualnego szablonu dla każdego typu certyfikatu.

- Specjalny certyfikat Agenta rejestracji (EA) powinien zostać zainstalowany na urządzeniu z Serwerem administracyjnym, w repozytorium certyfikatów konta, z poziomu którego wykonywana jest integracja z PKI. Certyfikat Agenta rejestracji (EA) jest wystawiany przez administratora urzędu certyfikacji domeny (CA).

Konto, z poziomu którego wykonywana jest integracja z PKI, musi spełniać następujące kryteria.

- Jest to użytkownik domeny.

- Jest to lokalny administrator urządzenia z Serwerem administracyjnym, z poziomu którego została zainicjowana integracja z PKI.

- Posiada uprawnienie do *Zalogowania w trybie usługi*.

- Urządzenie z zainstalowanym Serwerem administracyjnym musiało być wcześniej uruchomione przynajmniej raz z poziomu tego konta w celu utworzenia trwałego profilu użytkownika.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (zwany również serwerem sieciowym) jest składnikiem Kaspersky Security Center. Serwer sieciowy został zaprojektowany do publikowania autonomicznych pakietów instalacyjnych, autonomicznych pakietów instalacyjnych dla urządzeń mobilnych oraz plików z folderu współdzielonego.

Pakiety instalacyjne są automatycznie publikowane na serwerze sieciowym, a następnie są usuwane po pierwszym pobraniu. Administrator może wysłać użytkownikowi nowy odnośnik w dowolny sposób, na przykład za pośrednictwem poczty elektronicznej.

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

Ustawienia serwera sieciowego

Jeśli wymagane jest dostrojenie serwera WWW, jego właściwości umożliwiają zmiany portów dla HTTP (8060) i HTTPS (8061). Oprócz zmiany portów, możesz zastąpić certyfikat serwera dla HTTPS i zmienić FQDN serwera sieciowego dla HTTP.

Inne podstawowe prace

Ta sekcja zawiera zalecenia dotyczące codziennej pracy z Kaspersky Security Center.

Kolory ikony wskaźnika w Konsoli administracyjnej

Konsola administracyjna umożliwia szybką ocenę bieżącego stanu Kaspersky Security Center i zarządzanych urządzeń poprzez sprawdzenie wskaźników przypominających sygnalizację świetlną. Kolory wskaźnika są pokazywane w obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Monitorowanie**. Zakładka udostępnia sześć paneli informacyjnych ze wskaźnikami. Wskaźnik to kolorowy, pionowy pasek po lewej stronie panelu. Każdy panel ze wskaźnikiem odpowiada określonym zakresom funkcjonalnym Kaspersky Security Center (patrz tabela poniżej).

Kolory ikony wskaźnika w Konsoli administracyjnej

Nazwa panelu	Zakres funkcji
Wdrażanie	Instalacja Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci organizacji
Schemat zarządzania	Struktura grup administracyjnych. Skanowanie sieci. Reguły przenoszenia urządzeń
Ustawienia ochrony	Funkcjonalność aplikacji zabezpieczającej: stan ochrony, skanowanie w poszukiwaniu złośliwego oprogramowania
Aktualizacja	Uaktualnienia i łaty
Monitorowanie	Stan ochrony
Serwer administracyjny	Funkcje Serwera administracyjnego i właściwości

Każdy wskaźnik może przyjąć jeden z pięciu kolorów (patrz tabela poniżej). Kolor wskaźnika zależy od aktualnego stanu Kaspersky Security Center i zdarzeń, które zostały zarejestrowane.

Kolory zestawów

Stan	Kolor wskaźnika	Znaczenie koloru wskaźnika
Informacja	Zielony	Nie jest wymagana interwencja administratora.
Ostrzeżenie	Żółty	Wymagana jest interwencja administratora.
Krytyczny	Czerwony	Wystąpiły poważne problemy. W celu rozwiązania tych problemów wymagana jest interwencja administratora.
Informacja	Niebieski	Wydarzenia, które zostały zarejestrowane, nie są związane z potencjalnymi lub rzeczywistymi zagrożeniami dla bezpieczeństwa zarządzanych urządzeń.
Informacja	Szary	Szczegóły zdarzeń są niedostępne lub nie zostały jeszcze pobrane.

Celem administratora jest zachowanie zielonych kolorów wskaźników na wszystkich panelach informacyjnych, na zakładce **Monitorowanie**.

Zdalny dostęp do zarządzanych urządzeń

Ta sekcja zawiera informacje o zdalnym dostępie do zarządzanych urządzeń.

Korzystanie z opcji „Nie odłączaj od Serwera administracyjnego” w celu zapewnienia ciągłej łączności między zarządzanym urządzeniem a Serwerem administracyjnym

Jeśli nie używasz serwerów push, Kaspersky Security Center nie zapewnia ciągłej łączności między zarządzanymi urządzeniami a Serwerem administracyjnym. Agenty sieciowe na zarządzanych urządzeniach okresowo nawiązują połączenie i synchronizują się z Serwerem administracyjnym. Przerwa między tymi synchronizacjami jest definiowana w zasadzie Agenta sieciowego. Jeśli wymagana jest wczesna synchronizacja, Serwer administracyjny (lub punkt dystrybucji, jeśli jest w użyciu) wysyła podpisany pakiet sieciowy poprzez sieć IPv4 lub IPv6 do portu UDP Agenta sieciowego. Domyślnym numerem portu jest 15000. Jeśli nie jest możliwe nawiązanie połączenia między Serwerem administracyjnym a zarządzanym urządzeniem przy użyciu UDP, synchronizacja zostanie uruchomiona przy następnym regularnym połączeniu Agenta sieciowego z Serwerem administracyjnym w trakcie okresu synchronizacji.

Niektórych operacji nie można wykonać bez wcześniejszego nawiązania połączenia między Agentem sieciowym a Serwerem administracyjnym, takich jak uruchamianie i zatrzymywanie zadań lokalnych, odbieranie statystyk dla zarządzanej aplikacji lub tworzenie tunelu. Aby rozwiązać ten problem, jeśli nie korzystasz z serwerów push, możesz użyć opcji **Nie odłączaj od Serwera administracyjnego**, aby upewnić się, że istnieje ciągła łączność między zarządzanym urządzeniem a serwerem administracyjnym.

W celu zapewnienia ciągłego połączenia między zarządzanym urządzeniem a Serwerem administracyjnym:

1. Wykonaj jedną z poniższych czynności:

   - Jeśli zarządzane urządzenie uzyskuje dostęp do Serwera administracyjnego bezpośrednio (to znaczy nie za pośrednictwem punktu dystrybucji):

     a. W drzewie konsoli wybierz folder **Zarządzane urządzenia**.

     b. W obszarze roboczym folderu wybierz zarządzane urządzenie, z którym chcesz zapewnić ciągłą łączność.

     c. Z otwartego menu kontekstowego urządzenia wybierz **Właściwości**.

     Zostanie otwarte okno właściwości wybranego urządzenia.

   - Jeżeli zarządzane urządzenie uzyskuje dostęp do Serwera administracyjnego za pośrednictwem punktu dystrybucji działającego w trybie bramy, a nie bezpośrednio:

     a. W drzewie konsoli wybierz węzeł **Serwer administracyjny**.

     b. Z otwartego menu kontekstowego węzła wybierz **Właściwości**.

     c. W otwartym oknie właściwości Serwera administracyjnego wybierz sekcję **Punkty dystrybucji**.

     d. Na liście wybierz żądany punkt dystrybucji, a następnie kliknij **Właściwości**.

     Zostanie otwarte okno właściwości punktu dystrybucji.

2. W sekcji **Ogólny** wyświetlanego okna wybierz opcję **Nie odłączaj od Serwera administracyjnego**.

Trwałe połączenie jest nawiązywane między zarządzanym urządzeniem a Serwerem administracyjnym.

Maksymalna całkowita liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego** to 300.

Informacje o sprawdzaniu czasu połączenia pomiędzy urządzeniem a Serwerem administracyjnym

Po wyłączeniu urządzenia, Agent sieciowy powiadamia Serwer administracyjny o tym zdarzeniu. W Konsoli administracyjnej to urządzenie jest wyświetlane jako wyłączone. Jednakże Agent sieciowy nie może powiadamiać Serwera administracyjnego o wszystkich tego typu zdarzeniach. Dlatego też Serwer administracyjny okresowo analizuje atrybut **Połączono z Serwerem administracyjnym** (wartość tego atrybutu jest wyświetlana w Konsoli administracyjnej, we właściwościach urządzenia, w sekcji **Ogólny**) dla każdego urządzenia i porównuje go z interwałem synchronizacji z aktualnych ustawień Agenta sieciowego. Jeśli urządzenie nie odpowiedziało w ponad trzech pomyślnych interwałach synchronizacji, to urządzenie zostanie oznaczone jako wyłączone.

Informacje o wymuszonej synchronizacji

Chociaż Kaspersky Security Center automatycznie synchronizuje stan, ustawienia, zadania i profile dla zarządzanych urządzeń, to w niektórych przypadkach administrator musi dokładnie wiedzieć, czy dla określonego urządzenia w danym momencie została już przeprowadzona synchronizacja.

W menu kontekstowym zarządzanych urządzeń w Konsoli administracyjnej urządzenia element menu **Wszystkie zadania** zawiera polecenie **Wymuś synchronizację**. Jeśli Kaspersky Security Center 14.2 wykona to polecenie, Serwer administracyjny podejmie próbę nawiązania połączenia z urządzeniem. Jeśli ta próba zakończy się pomyślnie, zostanie wykonana wymuszona synchronizacja. W innym przypadku synchronizacja zostanie wymuszona dopiero po kolejnym zaplanowanym połączeniu nawiązanym pomiędzy Agentem sieciowym a Serwerem administracyjnym.

Informacje o tunelowaniu

Kaspersky Security Center umożliwia tunelowanie połączeń TCP z Konsoli administracyjnej poprzez Serwer administracyjny, a następnie poprzez Agenta sieciowego do określonego portu na zarządzanym urządzeniu. Tunelowanie połączeń jest przeznaczone dla połączenia aplikacji klienckiej na urządzeniu z zainstalowaną Konsolą administracyjną z portem TCP na zarządzanym urządzeniu—jeśli nie jest możliwe bezpośrednie połączenie między Konsolą administracyjną a urządzeniem docelowym.

Na przykład, tunelowanie jest wykorzystywane dla połączeń ze zdalnym pulpitem - zarówno do łączenia się z istniejącą sesją, jak i do tworzenia nowej zdalnej sesji.

Tunelowanie połączeń może zostać włączone także przy użyciu narzędzi zewnętrznych. Na przykład, administrator może uruchomić w ten sposób narzędzie putty, klienta VNC oraz inne narzędzia.

Podręcznik szacowania rozmiaru

Ta sekcja zawiera informacje na temat szacowania rozmiaru dla komponentów Kaspersky Security Center.

Informacje o podręczniku

Podręcznik szacowania rozmiaru dla Kaspersky Security Center 14.2 (zwany również Kaspersky Security Center) jest przeznaczony dla profesjonalistów, którzy instalują i zarządzają Kaspersky Security Center, a także dla tych, którzy zapewniają wsparcie techniczne organizacjom korzystającym z programu Kaspersky Security Center.

Wszystkie zalecenia i obliczenia zostały podane dla sieci, w których Kaspersky Security Center zarządza ochroną urządzeń z zainstalowanymi programami firmy Kaspersky, w tym urządzeniami mobilnymi. Jeśli urządzenia mobilne lub jakiekolwiek inne zarządzane urządzenia będą uwzględniane oddzielnie, zostanie to wyszczególnione.

Aby uzyskać i utrzymać optymalną wydajność w różnych warunkach pracy, należy wziąć pod uwagę liczbę urządzeń w sieci, topologię sieci oraz zestaw funkcji Kaspersky Security Center, jakich potrzebujesz.

Podręcznik zawiera następujące informacje:

- Ograniczenia Kaspersky Security Center
- Wyliczenia dla kluczowych węzłów Kaspersky Security Center (Serwerów administracyjnych i punktów dystrybucji):
  - Wymagania sprzętowe dla Serwerów administracyjnych i punktów dystrybucji
  - Obliczenie liczby i hierarchia Serwerów administracyjnych
  - Obliczenie liczby i konfiguracja punktów dystrybucji
- Konfiguracja rejestrowania zdarzeń w bazie danych w zależności od liczby urządzeń w sieci
- Konfiguracja określonych zadań mających na celu zapewnienie optymalnego działania Kaspersky Security Center
- Ilość ruchu sieciowego (obciążenie sieci) pomiędzy Serwerem administracyjnym Kaspersky Security Center a chronionym urządzeniem

Korzystanie z tego podręcznika jest zalecane w następujących przypadkach:

- Podczas rozplanowywania zasobów przed instalacją Kaspersky Security Center
- Podczas rozplanowywania istotnych zmian w sieci, w której wdrożony jest Kaspersky Security Center
- Jeśli przełączasz z używania Kaspersky Security Center w obrębie ograniczonego segmentu sieci (środowisko testowe) do wdrożenia Kaspersky Security Center na pełną skalę w sieci korporacyjnej
- Podczas wprowadzania zmian do zestawu używanych funkcji Kaspersky Security Center

Informacje o ograniczeniach Kaspersky Security Center

Poniższa tabela wyświetla ograniczenia bieżącej wersji Kaspersky Security Center.

Ograniczenia Kaspersky Security Center

Rodzaj ograniczenia	Wartość
Maksymalna liczba zarządzanych urządzeń na Serwer administracyjny	100 000
Maksymalna liczba urządzeń z wybraną opcją **Nie odłączaj od Serwera administracyjnego**	300
Maksymalna liczba grup administracyjnych	10 000
Maksymalna liczba przechowywanych zdarzeń	45 000 000
Maksymalna liczba profili	2000
Maksymalna liczba zadań	2000
Maksymalna całkowita liczba obiektów Active Directory (jednostek organizacyjnych i kont użytkowników, urządzeń oraz grup bezpieczeństwa)	1 000 000
Maksymalna liczba profili w zasadzie	100
Maksymalna liczba podrzędnych Serwerów administracyjnych w jednym głównym Serwerze administracyjnym	500
Maksymalna liczba wirtualnych Serwerów administracyjnych	500
Maksymalna liczba urządzeń, jaką obejmuje pojedynczy punkt dystrybucji (punkty dystrybucji mogą obejmować tylko urządzenia niemobilne)	10 000
Maksymalna liczba urządzeń, które mogą używać pojedynczej bramy połączenia	10 000, w tym urządzenia mobilne
Maksymalna liczba urządzeń mobilnych na Serwer administracyjny	100 000 minus liczba stacjonarnych zarządzanych urządzeń

Wyliczenia dla Serwerów administracyjnych

Ta sekcja zawiera wymagania programowe i sprzętowe dla urządzeń używanych jako Serwery administracyjne. Można tu znaleźć także zalecenia odnośnie wyliczania liczby i hierarchii Serwerów administracyjnych w zależności od konfiguracji sieci organizacji.

Obliczanie zasobów sprzętowych dla Serwera administracyjnego

Ta sekcja zawiera obliczenia pomagające w rozplanowaniu zasobów sprzętowych dla Serwera administracyjnego. Zalecenia dotyczące obliczenia przestrzeni dyskowej podczas korzystania z funkcji Zarządzanie lukami i poprawkami są dostępne oddzielnie.

Wymagania sprzętowe dla systemu zarządzania bazą danych i Serwera administracyjnego

W poniższej tabeli zostały uwzględnione zalecane minimalne wymagania sprzętowe dla DBMS i Serwera administracyjnego uzyskane w trakcie testów. Pełna lista obsługiwanych systemów operacyjnych i systemów DBMS znajduje się na liście wymagań sprzętowych i programowych.

Serwer administracyjny i DBMS znajdują się na różnych urządzeniach, sieć zawiera 50 000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym

Sprzęt	Wartość
Procesor	4 rdzenie, 2500 MHz
Pamięć RAM	8 GB
Dysk twardy	300 GB, zalecany RAID
Karta sieciowa	1 Gbit

Konfiguracja urządzenia z zainstalowanym DBMS

Sprzęt	Wartość
Procesor	4 rdzenie, 2500 MHz
Pamięć RAM	16 GB
Dysk twardy	200 GB, SATA RAID
Karta sieciowa	1 Gbit

Serwer administracyjny i DBMS znajdują się na tym samym urządzeniu, sieć zawiera 50 000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym i DBMS

Sprzęt	Wartość
Procesor	8 rdzeni, 2500 MHz
Pamięć RAM	16 GB
Dysk twardy	500 GB, SATA RAID
Karta sieciowa	1 Gbit

Serwer administracyjny i serwer SQL znajdują się na różnych urządzeniach, sieć zawiera 100 000 urządzeń

Konfiguracja urządzenia z zainstalowanym Serwerem administracyjnym

Sprzęt	Wartość
Procesor	8 rdzenie, 2,13 GHz
Pamięć RAM	8 GB
Dysk twardy	1 TB, RAID
Karta sieciowa	1 Gbit

Konfiguracja urządzenia z zainstalowanym serwerem DBMS

Sprzęt	Wartość
Procesor	8 rdzenie, 2,53 GHz
Pamięć RAM	26 GB
Dysk twardy	500 GB, SATA RAID
Karta sieciowa	1 Gbit

Testy zostały przeprowadzone z użyciem następujących ustawień:

- Automatyczne przydzielanie punktów dystrybucji jest włączone na Serwerze administracyjnym lub punkty dystrybucji są przydzielane ręcznie według zalecanej tabeli.
- Zadanie tworzenia kopii zapasowej zapisuje kopie zapasowe w zasobie plików znajdującym się na dedykowanym serwerze.
- Interwał synchronizacji dla Agentów sieciowych jest ustawiony w taki sposób, w jaki opisano to w poniższej tabeli.

Interwał synchronizacji dla Agentów sieciowych

Okres synchronizacji (minuty)	Liczba zarządzanych urządzeń
15	10 000
30	20 000
45	30 000
60	40 000
75	50 000
150	100 000

Obliczanie pojemności bazy danych

Przybliżoną ilość miejsca, jaką powinna zajmować baza danych, można obliczyć, korzystając z następującego wzoru:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

gdzie:

- C to liczba urządzeń.
- E to liczba przechowywanych zdarzeń.
- A to całkowita liczba obiektów Active Directory:
  - Konta urządzeń
  - Konta użytkowników
  - Konta grup bezpieczeństwa
  - Jednostki organizacyjne Active Directory

Jeśli skanowanie Active Directory jest wyłączone, zmienna A będzie równa zero.

- N to średnia liczba zinwentaryzowanych plików wykonywalnych na urządzeniu końcowym.
- F to liczba urządzeń końcowych, na których zinwentaryzowano pliki wykonywalne.

Jeśli planujesz włączyć w ustawieniach profilu Kaspersky Endpoint Security powiadamianie Serwera administracyjnego o aplikacjach, które uruchamiasz, będziesz potrzebował dodatkowej ilości (0,03 * C) gigabajtów do przechowywania w bazie danych informacji o aplikacjach, które uruchamiasz.

Jeśli Serwer administracyjny rozsyła aktualizacje systemu Windows (zachowując się przy tym jak serwer Windows Server Update Services), baza danych będzie wymagała dodatkowych 2,5 GB na dysku.

Podczas działania, w bazie danych zawsze znajduje się część *nieprzydzielonego obszaru*. Dlatego też, rzeczywisty rozmiar pliku bazy danych (domyślnie jest to plik KAV.MDF, jeśli jako DBMS używasz serwera SQL) okazuje się być około dwukrotnie większy niż ilość miejsca zajmowanego przez bazę danych.

Nie jest zalecane wyraźne ograniczenie rozmiaru dziennika transakcji (domyślnie, plik KAV_log.LDF, jeśli używasz serwera SQL jako systemu DBMS). Zalecane jest pozostawienie domyślnej wartości parametru MAXSIZE. Jednakże, jeśli musisz ograniczyć rozmiar tego pliku, weź pod uwagę fakt, że typowa niezbędna wartość parametru MAXSIZE dla KAV_log.LDF to 20480 MB.

Obliczanie przestrzeni dyskowej (z użyciem oraz bez użycia funkcji Zarządzanie lukami i poprawkami)

Obliczanie przestrzeni dyskowej bez użycia funkcji Zarządzanie lukami i poprawkami

Przestrzeń dyskowa na Serwerze administracyjnym, wymagana dla folderu %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit, może zostać oszacowana w przybliżeniu przy użyciu wzoru:

(724 * C + 0,15 * E + 0,17 * A), KB

gdzie:

- C to liczba urządzeń.
- E to liczba przechowywanych zdarzeń.
- A to całkowita liczba obiektów Active Directory:
  - Konta urządzeń
  - Konta użytkowników
  - Konta grup bezpieczeństwa
  - Jednostki organizacyjne Active Directory

Jeśli skanowanie Active Directory jest wyłączone, zmienna A będzie równa zero.

Obliczanie dodatkowej przestrzeni dyskowej z użyciem funkcji Zarządzanie lukami i poprawkami

- Uaktualnienia. Folder współdzielony dodatkowo potrzebuje przynajmniej 4 GB do przechowywania uaktualnień.
- Pakiety instalacyjne. Jeśli niektóre pakiety instalacyjne są przechowywane na Serwerze administracyjnym, folder współdzielony będzie wymagał dodatkowej ilości miejsca na dysku, równej całkowitemu rozmiarowi wszystkich dostępnych pakietów instalacyjnych przeznaczonych do zainstalowania.
- Zadania zdalnej instalacji. Jeśli zadania zdalnej instalacji znajdują się na Serwerze administracyjnym, wymagana będzie dodatkowa wolna przestrzeń na dysku (w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit) równa całkowitemu rozmiarowi wszystkich pakietów instalacyjnych przeznaczonych do zainstalowania.
- Poprawki. Jeśli Serwer administracyjny jest zaangażowany w instalację łat, niezbędna jest dodatkowa ilość wolnego miejsca na dysku:
  - Folder z poprawkami powinien posiadać ilość miejsca na dysku równą całkowitemu rozmiarowi wszystkich pobranych łat. Domyślnie, łaty są przechowywane w folderze %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (możesz użyć narzędzia klsrvswch do określenia innego folderu do przechowywania łat). Jeśli Serwer administracyjny jest używany jako serwer WSUS, zalecane jest przydzielenie temu folderowi przynajmniej 100 GB.
  - Folder %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit musi posiadać ilość miejsca na dysku równą całkowitemu rozmiarowi tych łat, do których odwołują się istniejące zadania instalacji aktualizacji (łat) i eliminacji luk.

Obliczanie liczby i konfigurowanie Serwerów administracyjnych

Aby zmniejszyć obciążenie na głównym Serwerze administracyjnym, do każdej grupy administracyjnej możesz przypisać oddzielny Serwer administracyjny. Liczba podrzędnych Serwerów administracyjnych nie może przekraczać 500 dla jednego głównego Serwera administracyjnego.

Zalecane jest utworzenie konfiguracji Serwerów administracyjnych w odniesieniu do konfiguracji sieci organizacji.

Zalecenia dotyczące łączenia dynamicznych maszyn wirtualnych z Kaspersky Security Center

Dynamiczne maszyny wirtualne (nazywane również dynamicznymi maszynami wirtualnymi) zużywają więcej zasobów niż statyczne maszyny wirtualne.

Aby uzyskać więcej informacji na temat dynamicznych maszyn wirtualnych, zobacz Obsługa dynamicznych maszyn wirtualnych.

Po podłączeniu nowej dynamicznej maszyny wirtualnej Kaspersky Security Center tworzy ikonę dla tej dynamicznej maszyny wirtualnej w Konsoli administracyjnej i przenosi dynamiczną maszynę wirtualną do grupy administracyjnej. Następnie dynamiczna maszyna wirtualna jest dodawana do bazy danych Serwera administracyjnego. Serwer administracyjny jest w pełni zsynchronizowany z Agentem sieciowym zainstalowanym na tej dynamicznej maszynie wirtualnej.

W sieci organizacji Agent sieciowy tworzy następujące listy sieci dla każdej dynamicznej maszyny wirtualnej:

- Sprzęt
- Zainstalowane oprogramowanie

- Wykryte luki w zabezpieczeniach
- Zdarzenia i listy plików wykonywalnych komponentu Kontrola aplikacji

Agent sieciowy przesyła te listy sieciowe do Serwera administracyjnego. Rozmiar list sieciowych zależy od komponentów zainstalowanych na dynamicznej maszynie wirtualnej i może wpływać na wydajność Kaspersky Security Center i systemu zarządzania bazami danych (DBMS). Należy zauważyć, że obciążenie może rosnąć nieliniowo.

Po zakończeniu pracy z dynamiczną maszyną wirtualną przez użytkownika i wyłączeniu jej, maszyna ta jest następnie usuwana z infrastruktury wirtualnej, a wpisy dotyczące tej maszyny są usuwane z bazy danych Serwera administracyjnego.

Wszystkie te działania zużywają dużo zasobów bazy danych Kaspersky Security Center i Serwera administracyjnego i mogą zmniejszyć wydajność Kaspersky Security Center i DBMS. Zalecamy podłączenie do 20 000 dynamicznych maszyn wirtualnych do Kaspersky Security Center.

Możesz podłączyć ponad 20 000 dynamicznych maszyn wirtualnych do Kaspersky Security Center, jeśli połączone dynamiczne maszyny wirtualne wykonują standardowe operacje (na przykład aktualizacje baz danych) i zużywają nie więcej niż 80 procent pamięci i 75–80 procent dostępnych rdzeni.

Zmiana ustawień zasad, oprogramowania lub systemu operacyjnego na dynamicznej maszynie wirtualnej może zmniejszyć lub zwiększyć zużycie zasobów. Za optymalne uważa się zużycie 80–95 procent zasobów.

Wyliczenia dla punktów dystrybucji i bram połączenia

Ta sekcja zawiera wymagania sprzętowe dla urządzeń używanych jako punkty dystrybucji wraz z zaleceniami dotyczącymi obliczenia liczby punktów dystrybucji i bram połączenia w zależności od konfiguracji sieci firmowej.

Wymagania wobec punktu dystrybucji

W celu zarządzania maksymalnie 10 000 urządzeń klienckich, punkt dystrybucji musi spełniać przynajmniej następujące wymagania (dostępna jest konfiguracja dla środowiska test stand):

- Procesor: Intel® Core™ i7-7700 CPU, 3.60 GHz 4 rdzenie.
- Pamięć RAM: 8 GB.
- Dysk: SSD 120 GB.

Dodatkowo, punkt dystrybucji musi posiadać dostęp do internetu i musi być zawsze podłączony.

Jeśli jakiekolwiek zadanie zdalnej instalacji jest oczekujące na Serwerze administracyjnym, urządzenie z zainstalowanym punktem dystrybucji będzie także wymagało wolnej przestrzeni na dysku równej całkowitemu rozmiarowi pakietów instalacyjnych przeznaczonych do zainstalowania.

Jeśli na Serwerze administracyjnym jest oczekujące jedno lub kilka zadań instalacji uaktualnień (łat) i naprawy luk, urządzenie z zainstalowanym punktem dystrybucji będzie także wymagało dodatkowej wolnej przestrzeni na dysku równej podwojonej wartości całkowitego rozmiaru wszystkich łat przeznaczonych do zainstalowania.

Obliczanie liczby i konfigurowanie punktów dystrybucji

Im więcej urządzeń klienckich zawiera sieć, tym więcej punktów dystrybucji wymaga. Nie jest zalecane wyłączanie automatycznego przypisywania punktów dystrybucji. Jeśli automatyczne przypisywanie punktów dystrybucji jest włączone, Serwer administracyjny przypisuje punkty dystrybucji, gdy liczba urządzeń klienckich jest dosyć duża, oraz definiuje ich konfigurację.

Używanie specjalnie przypisanych punktów dystrybucji

Jeśli planujesz używać określonych urządzeń jako punktów dystrybucji (na przykład, specjalnie wybranych serwerów), możesz zrezygnować z automatycznego przypisywania punktów dystrybucji. W tym przypadku upewnij się, że na urządzeniach, które mają pełnić rolę punktów dystrybucji, jest wystarczająca ilość wolnego miejsca, nie są regularnie wyłączane, a tryb uśpienia jest na nich wyłączony.

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Liczba specjalnie przypisanych punktów dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)
10–100	1
Więcej niż 100	Dopuszczalne: (N/10 000 + 1), zalecane: (N/5000 + 2), gdzie N to liczba urządzeń w sieci

Korzystanie ze standardowych urządzeń klienckich (stacji roboczych) jako punktów dystrybucji

Jeśli planujesz używać standardowych urządzeń klienckich (czyli stacji roboczych) jako punktów dystrybucji, zalecane jest przypisanie punktów dystrybucji w sposób pokazany w tabelach poniżej, aby uniknąć nadmiernego obciążenia kanałów komunikacji i Serwera administracyjnego:

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera pojedynczy segment sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich w segmencie sieci	Liczba punktów dystrybucji
Mniej niż 300	0 (nie przypisuj punktów dystrybucji)
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Liczba stacji roboczych działających jako punkty dystrybucji w sieci, która zawiera kilka segmentów sieci w oparciu o liczbę urządzeń w sieci

Liczba urządzeń klienckich na segment sieci	Liczba punktów dystrybucji
Mniej niż 10	0 (nie przypisuj punktów dystrybucji)

10–30	1
31–300	2
Więcej niż 300	(N/300 + 1), gdzie N oznacza liczbę urządzeń w sieci; muszą być przynajmniej 3 punkty dystrybucji

Jeśli punkt dystrybucji jest wyłączony (lub z jakiegoś powodu niedostępny), zarządzane urządzenia w tym obszarze mogą uzyskać dostęp do Serwera administracyjnego w celu pobrania uaktualnień.

Obliczanie liczby bram połączenia

Jeśli planujesz używać bramy połączenia, zalecane jest wskazanie specjalnego urządzenia do pełnienia tej funkcji.

Brama połączenia może obejmować maksymalnie 10 000 zarządzanych urządzeń, w tym urządzeń mobilnych.

Zapisywanie informacji o zdarzeniach dla zadań i profili

Ta sekcja zawiera wyliczenia związane z przechowywaniem zdarzeń w bazie danych Serwera administracyjnego i oferuje zalecenia dotyczące zminimalizowania liczby zdarzeń, co pozwala zmniejszyć obciążenie na Serwerze administracyjnym.

Domyślnie, właściwości każdego zadania i profilu zapewniają przechowywanie wszystkich zdarzeń związanych z wykonywaniem zadań i wymuszeniem profilu.

Jednakże, jeśli zadanie jest uruchamiane dość często (na przykład, więcej niż raz w tygodniu) i na całkiem dużej liczbie urządzeń (na przykład, więcej niż 10 000), liczba zdarzeń może okazać się zbyt duża i zdarzenia mogą wypełnić bazę danych. W tym przypadku zalecane jest wybranie jednej z dwóch opcji w ustawieniach zadania:

- **Zapisz zdarzenia dotyczące postępu zadania**. W tym przypadku baza danych pobiera tylko informacje o uruchomieniu zadania, postępie i zakończeniu (pomyślnie, z ostrzeżeniem lub błędem) z każdego urządzenia, na którym zadanie jest uruchomione.

- **Zapisz jedynie wyniki wykonywania zadania**. W tym przypadku baza danych pobiera tylko informacje o zakończeniu zadania (pomyślnie, z ostrzeżeniem lub błędem) z każdego urządzenia, na którym zadanie jest uruchomione.

Jeśli profil został zdefiniowany dla całkiem dużej liczby urządzeń (na przykład, więcej niż 10 000), liczba zdarzeń może okazać się zbyt duża i zdarzenia mogą wypełnić bazę danych. W tym przypadku zalecane jest wybranie tylko najbardziej krytycznych zdarzeń w ustawieniach profilu i włączenie ich zapisywania. Zalecane jest wyłączenie zapisywania wszystkich pozostałych zdarzeń.

Postępując w ten sposób, zmniejszysz liczbę zdarzeń w bazie danych, zwiększysz prędkość wykonywania scenariuszy skojarzonych z analizą tabeli zdarzeń w bazie danych, a także zmniejszysz ryzyko nadpisania krytycznych zdarzeń przez dużą liczbę zdarzeń.

Możesz także skrócić okres przechowywania zdarzeń skojarzonych z zadaniem lub profilem. Domyślny okres wynosi 7 dni dla zdarzeń związanych z zadaniem oraz 30 dni dla zdarzeń związanych z profilem. Podczas zmiany okresu przechowywania zdarzeń należy uwzględnić procedury obowiązujące w organizacji oraz czas, jaki administrator systemu może poświęcić na przeanalizowanie każdego zdarzenia.

Zmodyfikowanie ustawień przechowywania zdarzeń jest zalecane w następujących przypadkach:

- Zdarzenia dotyczące zmian w stanach pośrednich zadań grupowych oraz zdarzenia dotyczące stosowania profili zajmują dużą część wszystkich zdarzeń w bazie danych Kaspersky Security Center.
- Dziennik zdarzeń aplikacji Kaspersky zaczyna wyświetlać wpisy o automatycznym usuwaniu zdarzeń, gdy przekroczony zostanie ustawiony limit całkowitej liczby zdarzeń przechowywanych w bazie danych.

Wybierz opcje zapisywania zdarzeń w oparciu o założenie, że optymalna liczba zdarzeń pochodzących z jednego urządzenia w ciągu dnia nie może przekraczać 20. Jeśli to konieczne, możesz delikatnie zwiększyć ten limit, ale tylko wtedy, gdy liczba urządzeń w sieci jest relatywnie mała (mniej niż 10 000).

Szczególne względy i optymalne ustawienia określonych zadań

Niektóre zadania podlegają szczególnym zasadom dotyczącym liczby urządzeń w sieci. Ta sekcja oferuje zalecenia odnośnie optymalnej konfiguracji ustawień takich zadań.

Wyszukiwanie urządzeń, zadanie tworzenia kopii zapasowej danych, zadanie konserwacji baz danych oraz grupowe zadania aktualizacji Kaspersky Endpoint Security są częścią podstawowej funkcjonalności Kaspersky Security Center.

Zadanie inwentaryzacji jest częścią funkcji Zarządzanie lukami i poprawkami i jest niedostępne, jeśli ta funkcja nie została aktywowana.

Częstotliwość wykrywania urządzeń

Nie jest zalecane zwiększanie domyślnej częstotliwości wyszukiwania urządzeń, gdyż może to spowodować znaczne obciążenie kontrolerów domeny. Natomiast zalecane jest skonfigurowanie terminarza przeszukiwania z minimalną możliwą częstotliwością dozwoloną przez potrzeby organizacji. Zalecenia dotyczące obliczenia optymalnego terminarza znajdują się w tabeli poniżej.

Terminarz wyszukiwania urządzeń

Liczba urządzeń w sieci	Zalecana częstotliwość wyszukiwania urządzeń
Mniej niż 10 000	Domyślna częstotliwość lub mniejsza
10 000 lub większa	Raz dziennie lub rzadziej

Zadanie tworzenia kopii zapasowej danych Serwera administracyjnego i zadanie konserwacji baz danych

Serwer administracyjny przestaje działać podczas wykonywania następujących zadań:

- Tworzenie kopii zapasowych danych Serwera administracyjnego
- Konserwacja baz danych

Podczas wykonywania tych zadań baza danych nie może pobierać żadnych danych.

Konieczna może okazać się zmiana terminarza uruchamiania tych zadań, aby nie były uruchamiane w tym samym czasie co inne zadania Serwera administracyjnego.

Grupowe zadania aktualizacji Kaspersky Endpoint Security

Jeśli Serwer administracyjny pełni rolę źródła uaktualnień, zalecana opcja terminarza dla grupowych zadań aktualizacji Kaspersky Endpoint Security 10 i nowszych wersji to **Po pobraniu nowych uaktualnień do repozytorium** z zaznaczonym polem **Używaj automatycznie losowego opóźnienia dla uruchamiania zadań**.

Jeśli lokalne zadanie pobierania uaktualnień z serwerów Kaspersky do repozytorium jest tworzone na każdym punkcie dystrybucji, okresowe planowanie jest zalecane dla grupowego zadania aktualizacji Kaspersky Endpoint Security. W tym przypadku okres randomizacji musi wynosić jedną godzinę.

Zadanie Inwentaryzacja oprogramowania

Możesz zmniejszyć obciążenie bazy danych, jednocześnie uzyskując informacje o zainstalowanych aplikacjach. W tym celu zalecamy uruchomienie zadania inwentaryzacji na urządzeniach referencyjnych, na których jest zainstalowany standardowy zestaw oprogramowania.

Liczba plików wykonywalnych pobranych przez Serwer administracyjny z jednego urządzenia nie może przekraczać 150 000. Jeśli Kaspersky Security Center osiągnie ten limit, nie będzie mógł otrzymywać nowych plików.

Zazwyczaj liczba plików na standardowym urządzeniu klienckim nie przekracza 60 000. Liczba plików wykonywalnych na serwerze plików może być większa, a nawet przekraczać wartość progową wynoszącą 150 000.

Pomiary testowe wykazały, że zadanie inwentaryzacji zwraca następujące wyniki na urządzeniach działających pod kontrolą systemu operacyjnego Windows 7 z zainstalowanym programem Kaspersky Endpoint Security 11 i bez aplikacji innych producentów:

- Przy odznaczonych polach **Inwentaryzacja modułów DLL** i **Inwentaryzacja plików skryptu**: około 3 000 plików.
- Przy zaznaczonych polach **Inwentaryzacja modułów DLL** i **Inwentaryzacja plików skryptu**: od 10 000 do 20 000 plików w zależności od liczby zainstalowanych dodatków service pack dla systemu operacyjnego.
- Przy zaznaczonym polu **Inwentaryzacja plików skryptu**: około 10 000 plików.

Szczegóły dotyczące obciążenia sieci pomiędzy Serwerem administracyjnym a chronionymi urządzeniami

Ta sekcja zawiera wyniki pomiarów testowych ruchu sieciowego wraz z opisem warunków, w jakich te pomiary były robione. Możesz użyć tych informacji podczas planowania infrastruktury sieci i przepustowości sieci w organizacji (lub pomiędzy Serwerem administracyjnym a inną organizacją z urządzeniami, które mają być chronione). Znając przepustowość sieci, możesz w przybliżeniu oszacować czas potrzebny na przesłanie różnych danych.

Zużycie ruchu sieciowego w różnych scenariuszach

Poniższa tabela przedstawia wyniki testów pomiarowych ruchu sieciowego pomiędzy Serwerem administracyjnym a zarządzaną aplikacją w różnych scenariuszach.

Domyślnie, urządzenia są synchronizowane z Serwerem administracyjnym co 15 minut lub w dłuższych odstępach czasu. Jednakże, jeśli zmodyfikujesz ustawienia profilu lub zadania na Serwerze administracyjnym, wczesna synchronizacja będzie miała miejsce na urządzeniach, do których profil (lub zadanie) ma zastosowanie, aby nowe ustawienia zostały przesłane na te urządzenia.

Ilość ruchu sieciowego między Serwerem administracyjnym a zarządzanym urządzeniem

Scenariusz	Ruch sieciowy z Serwera administracyjnego do każdego zarządzanego urządzenia	Ruch sieciowy z każdego zarządzanego urządzenia do Serwera administracyjnego
Instalowanie Kaspersky Endpoint Security 11.7 for Windows z zaktualizowanymi bazami danych	390 MB	3.3 MB
Instalacja Agenta sieciowego	75 MB	397 KB
Równoległa instalacja Agenta sieciowego i Kaspersky Endpoint Security 11.7 for Windows	459 MB	3.6 MB
Wstępna aktualizacja antywirusowych baz danych bez aktualizowania baz danych w pakiecie (jeśli uczestnictwo w Kaspersky Security Network zostało wyłączone)	113 MB	1,8 MB
Codzienna aktualizacja antywirusowych baz danych (jeśli uczestnictwo w Kaspersky Security Network zostało włączone)	22 MB	373 MB
Wstępna synchronizacja przed zaktualizowaniem baz danych na urządzeniu (przesłanie profili i zadań)	382 KB	446 KB
Wstępna synchronizacja po aktualizacji baz danych na urządzeniu	20 KB	157 KB
Synchronizacja bez zmian na Serwerze administracyjnym (zgodnie z terminarzem)	18 KB	23 KB
Synchronizacja po zmianie jednego ustawienia w profilu grupowym (natychmiast po zmianie ustawienia)	19 KB	20 KB
Synchronizacja po zmianie jednego ustawienia w zadaniu grupowym (natychmiast po zmianie ustawienia)	14 KB	11 KB
Wymuszona synchronizacja	110 KB	109 KB
Zdarzenie **Wykryto wirusa** (1 wirus)	44 KB	50 KB
Zdarzenie **Wykryto wirusa** (10 wirusów)	58 KB	77 KB
Jednorazowy ruch po włączeniu listy Rejestr aplikacji	do 10 KB	do 12 KB
Codzienny ruch, gdy lista Rejestr aplikacji jest włączona	do 840 KB	do 1 MB

Przeciętne zużycie ruchu sieciowego w ciągu 24 godzin

Średnie 24-godzinne zużycie ruchu sieciowego między Serwerem administracyjnym a zarządzanym urządzeniem jest następujące:

- Ruch sieciowy z Serwera administracyjnego na zarządzane urządzenie wynosi 840 KB.
- Ruch sieciowy z zarządzanego urządzenia do Serwera administracyjnego wynosi 1 MB.

Ruch sieciowy mierzono w następujących warunkach:

- Na zarządzanym urządzeniu zainstalowano Agenta sieciowego i Kaspersky Endpoint Security 11.6 for Windows.
- Urządzenie nie zostało wskazane jako punkt dystrybucji.
- Funkcja Zarządzanie lukami i poprawkami nie została włączona.
- Częstotliwość synchronizacji z Serwerem administracyjnym wynosiło 15 minut.

Kontakt z działem pomocy technicznej

Ta sekcja opisuje sposób uzyskania pomocy technicznej oraz warunki, na jakich jest ona dostępna.

Jak uzyskać pomoc techniczną

Jeśli nie znajdziesz rozwiązania swojego problemu w dokumentacji do Kaspersky Security Center lub w jednym z dodatkowych źródeł informacji o Kaspersky Security Center, skontaktuj się z działem pomocy technicznej Kaspersky. Specjaliści z działu pomocy technicznej odpowiedzą na wszystkie pytania związane z instalacją i użytkowaniem Kaspersky Security Center.

Kaspersky zapewnia obsługę Kaspersky Security Center w trakcie jej cyklu życia (zajrzyj na stronę zawierającą czas trwania wsparcia technicznego produktu). Przed skontaktowaniem się z działem pomocy technicznej przeczytaj zasady korzystania z pomocy technicznej.

Możesz skontaktować się z działem pomocy technicznej na jeden z następujących sposobów:

- Odwiedzając witrynę pomocy technicznej
- Wysyłając zgłoszenie do pomocy technicznej poprzez portal Kaspersky CompanyAccount

Pomoc techniczna poprzez Kaspersky CompanyAccount

Kaspersky CompanyAccount jest to portal dla firm korzystających z aplikacji firmy Kaspersky. Portal Kaspersky CompanyAccount został zaprojektowany w celu ułatwienia interakcji między użytkownikami a specjalistami z Kaspersky poprzez zgłoszenia online. Możesz używać Kaspersky CompanyAccount do śledzenia stanu zgłoszeń online, a także przechowywać ich historię.

Możliwe jest zarejestrowanie wszystkich pracowników firmy pod jednym kontem w serwisie Kaspersky CompanyAccount. Jedno konto umożliwia scentralizowane zarządzanie zgłoszeniami elektronicznymi zarejestrowanych pracowników oraz zarządzanie uprawnieniami tych pracowników poprzez Kaspersky CompanyAccount.

Portal Kaspersky CompanyAccount jest dostępny w następujących językach:

- angielskim
- hiszpańskim
- włoskim
- niemieckim
- polskim
- portugalskim
- rosyjskim

- francuskim
- japońskim

Więcej informacji o Kaspersky CompanyAccount można znaleźć na stronie pomocy technicznej.

Źródła informacji o aplikacji

Strona Kaspersky Security Center na witrynie Kaspersky

Na stronie internetowej programu Kaspersky Security Center, dostępnej w witrynie Kaspersky znajdziesz ogólne informacje o aplikacji, jej funkcjach i właściwościach.

Strona Kaspersky Security Center w Bazie wiedzy

Baza wiedzy to sekcja na stronie działu pomocy technicznej Kaspersky.

Na stronie Kaspersky Security Center w Bazie wiedzy możesz przeczytać artykuły zawierające przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.

Artykuły w Bazie wiedzy mogą zawierać odpowiedzi na pytania dotyczące Kaspersky Security Center, a także innych aplikacji firmy Kaspersky. Artykuły w Bazie wiedzy mogą zawierać także nowości z działu pomocy technicznej.

Społeczność użytkowników produktów firmy Kaspersky

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, możesz przedyskutować je ze specjalistami z firmy Kaspersky lub z innymi użytkownikami na naszym Forum.

Na Forum możesz przeglądać istniejące tematy, pozostawiać swoje komentarze i tworzyć nowe tematy.

> Do przeglądania zasobów internetowych wymagane jest połączenie z internetem.

Jeśli nie możesz znaleźć rozwiązania swojego problemu, skontaktuj się z działem pomocy technicznej.

Słownik

Administrator dostawcy usługi

Pracownik u dostawcy usługi ochrony antywirusowej. Administrator wdraża i obsługuje systemy ochrony antywirusowej oparte na produktach antywirusowych firmy Kaspersky oraz zapewnia klientom pomoc techniczną.

Administrator klienta

Pracownik firmy klienta, który jest odpowiedzialny za stan ochrony antywirusowej i monitorowanie.

Agent autoryzacji

Interfejs umożliwiający przeprowadzenie procesu autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków twardych i załadowania systemu operacyjnego po zaszyfrowaniu dysku twardego.

Agent sieciowy

Składnik Kaspersky Security Center umożliwiający interakcję Serwera administracyjnego z aplikacjami firmy Kaspersky zainstalowanymi na określonym węźle sieciowym (stacji roboczej lub serwerze). Ten moduł jest wspólny dla wszystkich produktów Kaspersky dla Microsoft® Windows®. Oddzielne wersje Agenta sieciowego dostępne są dla aplikacji Kaspersky przeznaczonych dla systemów Unix i macOS.

Aktywny klucz

Klucz, który jest aktualnie używany przez aplikację.

Amazon Machine Image (AMI)

Szablon zawierający konfigurację oprogramowania niezbędną do uruchomienia maszyny wirtualnej. W oparciu o jeden obraz AMI można utworzyć kilka instancji.

Antywirusowe bazy danych

Bazy danych zawierają opisy zagrożeń ochrony komputera znane specjalistom z Kaspersky w momencie opublikowania antywirusowych baz danych. Wpisy w antywirusowych bazach danych pozwalają na wykrywanie szkodliwego kodu w skanowanych obiektach. Antywirusowe bazy danych są tworzone przez specjalistów z Kaspersky i aktualizowane co godzinę.

AWS API (Application Program Interface)

Interfejs programistyczny aplikacji platformy AWS, który jest używany przez Kaspersky Security Center. Narzędzia AWS API są przede wszystkim używane do przeszukiwania segmentu chmury i instalowania Agenta sieciowego na instancjach.

Bezpośrednie zarządzanie aplikacjami

Zarządzanie aplikacją poprzez interfejs lokalny.

Brama połączenia

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

Certyfikat współdzielony

Certyfikat, który jest przeznaczony do identyfikacji urządzenia mobilnego użytkownika.

Certyfikatu Serwera administracyjnego

Certyfikat używany przez Serwer administracyjny do następujących celów:

- Uwierzytelnianie Serwera administracyjnego podczas nawiązywania połączenia z Konsolą administracyjną opartą na MMC lub Konsolą Kaspersky Security Center Web Console
- Bezpieczna interakcja pomiędzy Serwerem administracyjnym a Agentami sieciowymi na zarządzanych urządzeniach
- Uwierzytelnianie Serwerów administracyjnych podczas łączenia głównego Serwera administracyjnego z dodatkowym Serwerem administracyjnym

Certyfikat jest tworzony automatycznie podczas instalacji Serwera administracyjnego, a następnie jest przechowywany na Serwerze administracyjnym.

Dodatkowy klucz subskrypcyjny

Klucz, który daje prawo do korzystania z aplikacji, chociaż nie jest on aktualnie w użyciu.

Domena rozgłoszeniowa

Logiczny obszar sieci, w której wszystkie węzły mogą wymieniać dane przy użyciu kanału informacyjnego na poziomie modelu OSI (Open Systems Interconnection Basic Reference Model).

Dostawca usługi ochrony antywirusowej

Firma, która oferuje organizacji klienta usługę ochrony antywirusowej opartą na rozwiązaniach firmy Kaspersky.

Dostępne aktualizacje

Zestaw uaktualnień dla modułów aplikacji firmy Kaspersky, w tym krytycznych aktualizacji zebranych przez pewien okres czasu oraz zmiany w architekturze aplikacji.

Epidemia wirusa

Seria celowych prób zainfekowania urządzenia wirusem.

Folder Kopia zapasowa

Specjalny folder do przechowywania kopii danych Serwera administracyjnego utworzonych przy użyciu narzędzia kopii zapasowej.

Grupa administracyjna

Zestaw urządzeń pogrupowanych według funkcji i zainstalowanych aplikacji firmy Kaspersky. Urządzenia są pogrupowane dla ułatwienia zarządzania nimi jako pojedynczą jednostką. Grupa może zawierać w sobie inne grupy. Zasady grupowe i zadania grupowe mogą być tworzone dla każdej zainstalowanej aplikacji w grupie.

Grupa licencjonowanych aplikacji

Grupa aplikacji utworzona w oparciu o kryterium ustalone przez administratora (na przykład, przez dostawcę), dla których zbierane są statystyki instalacji na urządzeniach klienckich.

Grupa ról

Grupa użytkowników urządzeń mobilnych z Exchange ActiveSync, którzy uzyskali podobne uprawnienia administracyjne.

HTTPS

Bezpieczny protokół używający szyfrowania do przesyłania danych między przeglądarką internetową a serwerem sieciowym. HTTPS jest używany w celu uzyskania dostępu do poufnych informacji, takich jak dane firmowe i finansowe.

Identity and Access Management (IAM)

Usługa AWS, która umożliwia zarządzanie dostępem użytkownika do innych zasobów i usług AWS.

Instalacja lokalna

Instalacja aplikacji zabezpieczającej na urządzeniu w sieci firmowej, która zakłada ręczne uruchomienie procesu instalacji z pakietu dystrybucyjnego aplikacji antywirusowej lub ręczne uruchomienie opublikowanego pakietu instalacyjnego, który wcześniej został pobrany na urządzenie.

Instalacja ręczna

Instalacja aplikacji zabezpieczającej na urządzeniu w sieci firmowej z pakietu dystrybucyjnego. Ręczna instalacja musi odbywać się z udziałem administratora lub innego specjalisty ds. IT. Zazwyczaj ręczna instalacja jest wykonywana wtedy, gdy zdalna instalacja zakończyła się błędem.

Instalacja wymuszona

Metoda zdalnej instalacji aplikacji Kaspersky, która umożliwia zainstalowanie oprogramowania na określonych urządzeniach klienckich. Aby instalacja wymuszona mogła być poprawnie przeprowadzona, konto używane dla tego zadania musi posiadać odpowiednie uprawnienia do zdalnego uruchamiania aplikacji na urządzeniach klienckich. Ta metoda jest zalecana do zainstalowania aplikacji na urządzeniach, które działają pod kontrolą systemów operacyjnych Microsoft Windows i obsługują tę funkcjonalność.

Instalacja zdalna

Instalacja aplikacji firmy Kaspersky przy użyciu usług oferowanych przez Kaspersky Security Center.

Instancja Amazon EC2

Maszyna wirtualna utworzona w oparciu o obraz AMI przy użyciu Amazon Web Services.

Istotność poprawki

Atrybut poprawki. Dla poprawek firmy Microsoft i poprawek firm trzecich istnieje pięć poziomów istotności:

- Krytyczny

- Wysoki
- Średni
- Niski
- Nieznany

Istotność poprawki firmy trzeciej lub firmy Microsoft jest determinowana przez najmniej preferowane priorytety wśród luk, które poprawka powinna wyeliminować.

JavaScript

Język programowania rozszerzający działanie stron internetowych. Strony internetowe utworzone przy użyciu JavaScript mogą wykonywać funkcje (na przykład zmieniać widok elementów interfejsu lub otwierać dodatkowe okna) bez konieczności odświeżania strony internetowej z nowymi danymi z serwera sieciowego. Aby przeglądać strony utworzone przy użyciu JavaScript, włącz obsługę JavaScript w ustawieniach swojej przeglądarki internetowej.

Kaspersky Private Security Network (KPSN)

Sieć Kaspersky Private Security Network to rozwiązanie, które daje użytkownikom urządzeń z zainstalowanymi aplikacjami firmy Kaspersky możliwość dostępu do baz danych reputacji Kaspersky Security Network i innych danych statystycznych bez wysyłania danych z ich urządzeń do Kaspersky Security Network. Sieć Kaspersky Private Security Network została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z jednego z następujących powodów:

- Urządzenia nie są podłączone do Internetu.
- Przesyłanie jakichkolwiek danych poza kraj lub firmową sieć LAN jest zabronione przez prawo lub politykę bezpieczeństwa firmy.

Administrator Kaspersky Security Center

Osoba zarządzająca działaniami aplikacji poprzez system scentralizowanej zdalnej administracji Kaspersky Security Center.

Kaspersky Security Center System Health Validator (SHV)

Składnik aplikacji Kaspersky Security Center, zaprojektowany do sprawdzania działania systemu operacyjnego w przypadku równoczesnego działania Kaspersky Security Center i Microsoft NAP.

Kaspersky Security Center Web Server

Komponent Kaspersky Security Center, który jest instalowany wraz z Serwerem administracyjnym. Serwer WWW został zaprojektowany do przesyłania za pośrednictwem sieci autonomicznych pakietów instalacyjnych, profili iOS MDM oraz plików z folderu współdzielonego.

Kaspersky Security Network (KSN)

Usługa chmury oferująca dostęp do bazy danych firmy Kaspersky, zawierającej ciągle aktualizowane informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji Kaspersky po wykryciu zagrożenia, ulepszenie działania niektórych składników ochrony oraz zmniejszenie ryzyka wystąpienia fałszywych alarmów.

Klient Serwera administracyjnego (urządzenie klienckie)

Urządzenie, serwer lub stacja robocza, na której zainstalowany jest Agent sieciowy i zarządzane aplikacje Kaspersky.

Klucz dostępu AWS IAM

Jest to kombinacja identyfikatora klucza (który wygląda jak "AKIAIOSFODNN7EXAMPLE") i klucza tajnego (który wygląda jak "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Ta para należy do użytkownika IAM i jest używana do uzyskania dostępu do usług AWS.

Konsola zarządzania AWS

Interfejs sieciowy do przeglądania i zarządzania zasobami AWS. Konsola zarządzania AWS jest dostępna na stronie https://aws.amazon.com/console/.

Konsola administracyjna

Składnik Kaspersky Security Center oparty na systemie Windows (zwany również Konsolą administracyjną opartą na MMC). Ten składnik zapewnia interfejs użytkownika dla usług administracyjnych Serwera administracyjnego i Agenta sieciowego.

Kopia zapasowa danych Serwera administracyjnego

Kopiowanie przy użyciu narzędzia kopii zapasowej danych Serwera administracyjnego do miejsca przechowywania oraz ich późniejsze przywracanie. Narzędzie to umożliwia zapisanie:

- Bazy danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym)
- Informacji o konfiguracji struktury grup administracyjnych i urządzeń klienckich
- Miejsc przechowywania plików instalacyjnych przeznaczonych do zdalnej instalacji aplikacji (zawartość folderów: Pakiety, Dezinstalacja uaktualnień)

- Certyfikatu Serwera administracyjnego

Luka

Jest to słaby punkt systemu operacyjnego lub aplikacji, który może zostać wykorzystany przez twórców szkodliwego oprogramowania w celu przeniknięcia do systemu operacyjnego lub aplikacji i naruszenia jego/jej integralności. Duża liczba luk w systemie operacyjnym świadczy o jego zawodności, gdyż wirusy, które przeniknęły do systemu, mogą powodować błędy w działaniu systemu i zainstalowanych aplikacjach.

Macierzysty Serwer administracyjny

Macierzysty Serwer administracyjny jest to Serwer administracyjny, który został określony podczas instalacji Agenta sieciowego. Macierzysty Serwer administracyjny może zostać użyty w ustawieniach profili połączenia Agenta sieciowego.

Niekompatybilna aplikacja

Aplikacja antywirusowa innego producenta lub aplikacja firmy Kaspersky, która nie obsługuje opcji zarządzania poprzez Kaspersky Security Center.

Ochrona antywirusowa sieci

Zestaw działań technicznych i firmowych, które zmniejszają prawdopodobieństwo przeniknięcia wirusów i spamu do sieci organizacji, a także blokują ataki sieciowe, phishing i inne zagrożenia. Ochrona sieci wzrasta, gdy używasz usług i aplikacji zabezpieczających i gdy stosujesz zasady ochrony danych firmowych.

Okres licencji

Przedział czasu, w którym masz dostęp do funkcji aplikacji i posiadasz uprawnienia do korzystania z dodatkowych usług. Zakres usług zależy od typu licencji.

Operator Kaspersky Security Center

Użytkownik monitorujący stan i działanie systemu ochrony zarządzanego poprzez Kaspersky Security Center.

Pakiet instalacyjny

Zestaw plików utworzonych dla zdalnej instalacji aplikacji Kaspersky przy pomocy systemu zdalnego zarządzania Kaspersky Security Center. Pakiet instalacyjny zawiera zakres ustawień potrzebnych do zainstalowania aplikacji i uruchomienia jej natychmiast po zainstalowaniu. Ustawienia odpowiadają domyślnym ustawieniom aplikacji. Pakiet instalacyjny jest tworzony przy użyciu plików z rozszerzeniami .kpd i .kud zawartych w pakiecie dystrybucyjnym aplikacji.

Plik klucza

Plik w formacie xxxxxxxx.key pozwala na korzystanie z aplikacji firmy Kaspersky na warunkach licencji testowej lub komercyjnej.

Priorytet zdarzenia

Cecha zdarzenia, które wystąpiło podczas działania aplikacji firmy Kaspersky. Dostępne są następujące priorytety:

- Zdarzenie krytyczne
- Błąd funkcjonalny
- Ostrzeżenie
- Informacja

Zdarzenia tego samego typu mogą posiadać różne poziomy priorytetu, w zależności od sytuacji, w której wystąpiły.

Profil

Zbiór ustawień urządzeń mobilnych Exchange określających ich zachowanie po podłączeniu do serwera Microsoft Exchange Server.

Profil informacyjny

Zbiór ustawień dotyczących działania aplikacji na urządzeniach mobilnych iOS. Profil informacyjny zawiera informacje o licencji; jest związany z określoną aplikacją.

Profil iOS MDM

Zbiór ustawień dotyczących łączenia urządzeń mobilnych iOS z Serwerem administracyjnym. Użytkownik instaluje profil iOS MDM na urządzeniu mobilnym, po czym to urządzenie mobilne łączy się z Serwerem administracyjnym.

Profil konfiguracyjny

Zasada zawierająca zbiór ustawień i ograniczeń dla urządzenia mobilnego iOS MDM.

Próg aktywności wirusa

Największa dozwolona liczba zdarzeń określonego typu w pewnym przedziale czasowym; przekroczenie tej wartości jest interpretowane jako wzrost aktywności wirusa i zagrożenie epidemią wirusa. Funkcja ta jest bardzo przydatna podczas okresów epidemii wirusów, gdyż daje administratorom możliwość reagowania w odpowiedniej chwili na zagrożenia ataku wirusów.

Przywracanie

Przeniesienie oryginalnego obiektu z kwarantanny lub folderu kopii zapasowej do folderu, w którym się znajdował przed umieszczeniem go w kwarantannie, wyleczeniem czy usunięciem, lub do folderu wskazanego przez użytkownika.

Przywrócenie danych Serwera administracyjnego

Przywrócenie danych Serwera administracyjnego z informacji zapisanej w kopii zapasowej przy pomocy narzędzia kopii zapasowej. Narzędzie to umożliwia przywrócenie:

- Bazy danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym)
- Informacji o konfiguracji struktury grup administracyjnych i komputerów klienckich
- Miejsc przechowywania plików instalacyjnych przeznaczonych do zdalnej instalacji aplikacji (zawartość folderów: Pakiety, Dezinstalacja uaktualnień)
- Certyfikatu Serwera administracyjnego

Punkt dystrybucji

Komputer, na którym został zainstalowany Agent sieciowy i który jest używany do rozsyłania uaktualnień, zdalnej instalacji aplikacji, uzyskiwania informacji o komputerach w grupie administracyjnej i/lub domenie rozgłoszeniowej. Punkty dystrybucji zostały utworzone w celu zmniejszenia obciążenia na Serwerze administracyjnym podczas dystrybucji uaktualnień i zoptymalizowania ruchu sieciowego. Punkty dystrybucji mogą być wskazywane automatycznie, przez Serwer administracyjny, lub ręcznie, przez administratora. Punkt dystrybucji był wcześniej znany jako agent aktualizacji.

Repozytorium zdarzeń

Część bazy danych Serwera administracyjnego przeznaczonej do przechowywania informacji o zdarzeniach, które występują w Kaspersky Security Center.

Rola IAM

Zestaw uprawnień do wykonywania żądań do usług opartych na AWS. Role IAM nie są skojarzone z określonym użytkownikiem lub grupą; zapewniają uprawnienia dostępu bez kluczy dostępu AWS IAM. Możesz przypisać rolę IAM do użytkowników IAM, instancji EC2 oraz usług i aplikacji opartych na AWS.

Scentralizowane zarządzanie aplikacjami

Zdalne zarządzanie aplikacją przy pomocy usług administracyjnych zawartych w Kaspersky Security Center.

Serwer administracyjny

Moduł aplikacji Kaspersky Security Center realizujący funkcje scentralizowanego przechowywania informacji na temat wszystkich aplikacji firmy Kaspersky zainstalowanych w sieci korporacyjnej. Może być używany do zarządzania tymi aplikacjami.

Serwer iOS MDM

Składnik Kaspersky Security Center zainstalowany na urządzeniu klienckim pozwalający na połączenie urządzeń mobilnych iOS z Serwerem administracyjnym za pośrednictwem usługi Apple Push Notifications (APN).

Serwer urządzeń mobilnych

Składnik Kaspersky Security Center umożliwiający dostęp do urządzeń mobilnych i zarządzanie nimi za pośrednictwem Konsoli administracyjnej.

Serwer urządzeń mobilnych Exchange

Składnik Kaspersky Security Center pozwalający na łączenie urządzeń mobilnych Exchange ActiveSync z Serwerem administracyjnym.

Serwery aktualizacji Kaspersky

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

Sklep aplikacji

Komponent Kaspersky Security Center. Sklep aplikacji jest używany do zainstalowania aplikacji na urządzeniach z systemem Android, należących do użytkownika. Sklep aplikacji umożliwia opublikowanie plików APK aplikacji oraz odnośników do aplikacji w Google Play.

Środowisko chmury

Maszyny wirtualne i inne zasoby wirtualne, które są oparte na platformie chmury i są połączone w sieci.

SSL

Protokół szyfrowania danych używany w internecie i sieciach lokalnych. Protokół Secure Sockets Layer (SSL) jest używany w aplikacjach internetowych do tworzenia bezpiecznego połączenia między klientem a serwerem.

Stacja robocza administratora

Urządzenie, na którym zainstalowana jest Konsola administracyjna lub którego używasz do otwierania Kaspersky Security Center Web Console. Ten komponent oferuje interfejs zarządzania Kaspersky Security Center.

Stacja robocza administratora służy do konfigurowania i zarządzania częścią serwerową Kaspersky Security Center. Korzystając ze stacji roboczej administratora, administrator tworzy i zarządza scentralizowanym systemem ochrony antywirusowej dla korporacyjnych sieci LAN opartych o aplikacje Kaspersky.

Stan ochrony

Bieżący stan ochrony, który odzwierciedla poziom ochrony komputera.

Stan ochrony sieci

Bieżący stan ochrony, który definiuje bezpieczeństwo urządzeń w sieci firmowej. Stan ochrony sieci uwzględnia takie czynniki, jak zainstalowane aplikacje zabezpieczające, użycie kluczy licencyjnych oraz liczba i typy wykrytych zagrożeń.

Strefa zdemilitaryzowana (DMZ)

Strefa zdemilitaryzowana jest segmentem sieci lokalnej zawierającej serwery, które odpowiadają na zapytania z sieci globalnej. Aby zapewnić bezpieczeństwo firmowej sieci lokalnej, dostęp do sieci LAN z poziomu strefy zdemilitaryzowanej jest chroniony przez zaporę sieciową.

Uprawnienia administracyjne

Poziom uprawnień użytkownika wymaganych do zarządzania obiektami Exchange w obrębie organizacji Exchange.

Urządzenie chronione UEFI

Urządzenie z programem Kaspersky Anti-Virus dla UEFI zintegrowanym na poziomie BIOS-u. Zintegrowana ochrona zapewnia bezpieczeństwo urządzenia od momentu uruchomienia systemu, natomiast ochrona na urządzeniach bez zintegrowanego oprogramowania zaczyna działać dopiero po uruchomieniu aplikacji zabezpieczającej.

Aktualizacja

Procedura zastępowania lub dodawania nowych plików (baz danych lub modułów aplikacji) pobieranych z serwerów aktualizacji firmy Kaspersky.

Urządzenie EAS

Urządzenie mobilne podłączone do Serwera administracyjnego za pośrednictwem protokołu Exchange ActiveSync. Urządzenia z systemami operacyjnymi iOS, Android i Windows Phone® mogą być podłączane i zarządzane poprzez protokół Exchange ActiveSync.

Urządzenie iOS MDM

Urządzenie mobilne, które jest podłączone do serwera iOS MDM poprzez protokół iOS MDM. Urządzenia działające pod kontrolą systemu operacyjnego iOS mogą być podłączane i zarządzane poprzez protokół iOS MDM.

Urządzenie KES

Urządzenie mobilne, które jest podłączone do Serwera administracyjnego i zarządzane poprzez Kaspersky Endpoint Security for Android.

Ustawienia programu

Ustawienia aplikacji, które są wspólne dla wszystkich typów zadań i zarządzają ogólnym działaniem aplikacji, na przykład, ustawienia działania aplikacji, ustawienia raportowania i ustawienia tworzenia kopii zapasowej.

Ustawienia zadania

Ustawienia aplikacji, które są specyficzne dla każdego typu zadania.

Użytkownicy wewnętrzni

Konta użytkowników wewnętrznych są używane do pracy z wirtualnymi Serwerami administracyjnymi. Kaspersky Security Center nadaje wewnętrznym użytkownikom aplikacji uprawnienia rzeczywistych użytkowników.

Konta wewnętrznych użytkowników są tworzone i używane tylko w obrębie Kaspersky Security Center. Do systemu operacyjnego nie są przesyłane żadne dane dotyczące wewnętrznych użytkowników. Kaspersky Security Center autoryzuje wewnętrznych użytkowników.

Użytkownik IAM

Użytkownik usług AWS. Użytkownik IAM może mieć uprawnienia do wykonywania przeszukiwania segmentu chmury.

Windows Server Update Services (WSUS)

Aplikacja wykorzystywana do rozpowszechniania aktualizacji dla aplikacji firmy Microsoft na komputerach użytkowników w sieci firmowej.

Wirtualny Serwer administracyjny

Składnik Kaspersky Security Center zaprojektowany do zarządzania systemem ochrony sieci organizacji klienta.

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

- Wirtualny Serwer administracyjny można utworzyć tylko na głównym Serwerze administracyjnym.
- Podczas działania wirtualny Serwer administracyjny używa bazy danych głównego Serwera administracyjnego. Zadania tworzenia kopii zapasowych i przywracania danych, a także zadania pobierania i skanowania aktualizacji nie są obsługiwane na wirtualnym Serwerze administracyjnym.
- Serwer wirtualny nie obsługuje tworzenia podrzędnych Serwerów administracyjnych (łącznie z Serwerami wirtualnymi).

Właściciel urządzenia

Właściciel urządzenia to użytkownik, z którym administrator może skontaktować się, gdy zajdzie potrzeba wykonania określonych działań na urządzeniu.

Wtyczka administracyjna

Specjalny moduł, który zawiera interfejs zarządzania aplikacją poprzez Konsolę administracyjną. Każda aplikacja posiada własną wtyczkę. Znajduje się ona we wszystkich aplikacjach firmy Kaspersky, które mogą być zarządzane przy użyciu Kaspersky Security Center.

Zadanie

Funkcje wykonywane przez aplikacje Kaspersky są zaimplementowane w postaci zadań, na przykład: Ochrona plików w czasie rzeczywistym, Pełne skanowanie komputera, Aktualizacja baz danych.

Zadanie dla określonych urządzeń

Zadanie przypisane do zbioru urządzeń klienckich z dowolnej grupy administracyjnej, wykonywane na tych urządzeniach.

Zadanie grupowe

Zadanie zdefiniowane dla grupy administracyjnej i wykonywane na wszystkich urządzeniach klienckich należących do tej grupy administracyjnej.

Zadanie lokalne

Zadanie utworzone i uruchomione na pojedynczym komputerze klienckim.

Zarządzane urządzenia

Urządzenia z sieci firmowej, które znajdują się w grupie administracyjnej.

Zasada

Zasada określa ustawienia aplikacji i zarządza możliwością konfigurowania tą aplikacją na komputerach w grupie administracyjnej. Dla każdej aplikacji należy utworzyć jedną zasadę. Możliwe jest utworzenie kilku zasad dla aplikacji zainstalowanych na komputerach w każdej grupie administracyjnej, ale tylko jedna zasada może być stosowana do każdej aplikacji w obrębie grupy administracyjnej w danym czasie.

Informacje o kodzie firm trzecich

Informacje o kodzie firm trzecich znajdują się w pliku legal_notices.txt, znajdującym się w folderze instalacyjnym aplikacji.

Informacje o znakach towarowych

Zastrzeżone znaki towarowe i usługowe stanowią odpowiednio własność ich właścicieli.

Adobe, Acrobat, Flash, Shockwave i PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe w Stanach Zjednoczonych i/lub innych krajach.

AMD, AMD64 są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace są znakami towarowymi firmy Amazon.com, Inc. lub jej podmiotów stowarzyszonych.

Apache oraz logo z piórem są zastrzeżonymi znakami towarowymi firmy Apache Software Foundation.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime i Touch ID są zastrzeżonymi znakami towarowymi firmy Apple Inc.

Arm jest zastrzeżonym znakiem towarowym firmy Arm Limited (lub jej spółek zależnych) w Stanach Zjednoczonych i/lub innych krajach.

Logo, marka i słowo Bluetooth należą do firmy Bluetooth SIG, Inc.

Ubuntu, LTS są zastrzeżonymi znakami towarowymi firmy Canonical Ltd.

Cisco Systems, Cisco, Cisco Jabber, IOS są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Cisco Systems, Inc. i/lub jej podmiotów w Stanach Zjednoczonych i innych krajach.

Citrix, XenServer są znakami towarowymi firmy Citrix Systems, Inc. i/lub jednego lub więcej oddziałów i mogą być zarejestrowane w Urzędzie patentowym w Stanach Zjednoczonych i innych krajach.

Corel jest zastrzeżonym znakiem towarowym bądź znakiem towarowym firmy Corel Corporation i/lub jej oddziałów w Kanadzie, Stanach Zjednoczonych i/lub innych krajach.

Cloudflare, logo Cloudflare i Cloudflare Workers są znakami towarowymi i/lub zastrzeżonymi znakami towarowymi firmy Cloudflare, Inc. w Stanach Zjednoczonych i innych jurysdykcjach.

Dropbox jest zastrzeżonym znakiem towarowym firmy Dropbox, Inc.

Radmin jest zastrzeżonym znakiem towarowym firmy Famatech.

Firebird jest zastrzeżonym znakiem towarowym firmy Firebird Foundation.

Foxit jest zastrzeżonym znakiem towarowym firmy Foxit Corporation.

FreeBSD jest zastrzeżonym znakiem towarowym firmy The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS i YouTube są zastrzeżonymi znakami towarowymi firmy Google LLC.

EulerOS, FusionCompute, FusionSphere są znakami towarowymi firmy Huawei Technologies Co., Ltd.

Intel, Core, Xeon są znakami towarowymi firmy Intel Corporation w Stanach Zjednoczonych i/lub innych krajach.

IBM, QRadar są znakami towarowymi firmy International Business Machines Corporation, zarejestrowanymi w wielu jurysdykcjach na świecie.

Node.js jest zastrzeżonym znakiem towarowym firmy Joyent, Inc.

Linux jest zastrzeżonym znakiem towarowym Linus Torvalds w Stanach Zjednoczonych i innych krajach.

Logitech jest zastrzeżonym znakiem towarowym lub znakiem towarowym firmy Logitech w Stanach Zjednoczonych i/lub innych krajach.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista, oraz Windows Azure są znakami towarowymi grupy firm Microsoft.

CVE jest zastrzeżonym znakiem towarowym The MITRE Corporation.

Mozilla, Firefox, Thunderbird są znakami towarowymi Mozilla Foundation w Stanach Zjednoczonych i innych krajach.

Novell jest zastrzeżonym znakiem towarowym firmy Novell Enterprises Inc. w Stanach Zjednoczonych i innych krajach.

NetWare jest zastrzeżonym znakiem towarowym firmy Novell, Inc. w Stanach Zjednoczonych i innych krajach.

Oracle, Java, JavaScript i TouchDown są zastrzeżonymi znakami towarowymi firmy Oracle i/lub jej oddziałów.

Parallels, logo Parallels i Coherence są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Parallels International GmbH.

Chef jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Progress Software Corporation i/lub jednym z jej oddziałów lub podmiotów, zarejestrowanym w Stanach Zjednoczonych i/lub innych krajach.

Puppet jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Puppet, Inc.

Python jest znakiem towarowym lub zastrzeżonym znakiem towarowym Python Software Foundation.

Red Hat, Fedora i Red Hat Enterprise Linux są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Red Hat, Inc. lub jej oddziałów, zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

Ansible jest zastrzeżonym znakiem towarowym firmy Red Hat, Inc. w Stanach Zjednoczonych i innych krajach.

CentOS jest znakiem towarowym lub zarejestrowanym znakiem towarowym firmy Red Hat, Inc. lub jej spółek zależnych w Stanach Zjednoczonych i innych krajach.

BlackBerry jest zastrzeżonym znakiem towarowym firmy Research In Motion Limited zarejestrowanym na terenie Stanów Zjednoczonych i jest w trakcie rejestrowania lub już jest zarejestrowany na terenie innych krajów.

SAMSUNG jest znakiem towarowym firmy SAMSUNG w Stanach Zjednoczonych i innych krajach.

Debian jest zastrzeżonym znakiem towarowym firmy Software in the Public Interest, Inc.

Splunk, SPL są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Splunk Inc., zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

SUSE jest zastrzeżonym znakiem towarowym firmy SUSE LLC, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

Symbian jest znakiem towarowym firmy Symbian Foundation Ltd.

OpenAPI to znak towarowy firmy The Linux Foundation.

VMware, VMware vSphere, VMware Workstation są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy VMware, Inc., zarejestrowanymi w Stanach Zjednoczonych i/lub innych jurysdykcjach.

UNIX jest zastrzeżonym znakiem towarowym w Stanach Zjednoczonych i innych krajach, używanym na wyłącznej licencji firmy X/Open Company Limited.

Zabbix jest zastrzeżonym znakiem towarowym firmy Zabbix SIA.

Znane problemy

Kaspersky Security Center Web Console ma szereg ograniczeń, które nie są krytyczne dla działania aplikacji:

- Jeśli lista zawiera więcej niż 20 elementów (w tym przypadku elementy są wyświetlane na kilku stronach) i zaznaczysz pole wyboru **Zaznacz wszystko**, w programie Web Console zostaną zaznaczone tylko elementy wyświetlane na bieżącej stronie.
- Po zakończeniu *skanowania IOC* zadania lokalnego stan zadania jest wyświetlany jako *Zaplanowane*.
- Urządzenia klienckie mogą nie zostać znalezione po uruchomieniu sondowania sieci systemu Windows.
- W profilu Kaspersky Endpoint Security for Windows, jeśli wybierzesz i zastosujesz kategorię aplikacji podczas konfigurowania funkcji Kontroli aplikacji, kategoria zostanie zastosowana, ale nie będzie wyświetlana jako wybrana po zapisaniu i ponownym otwarciu profilu.
- Po wyłączeniu usługi KSN Proxy stan urządzeń w grupie Zarządzane urządzenia zmienia się na *Krytyczny*, ale urządzenia w podgrupach są wyświetlane ze stanem *OK*.
- Jeśli dla bazy danych używanej przez Kaspersky Security Center ustawione jest sortowanie z rozróżnianiem wielkości liter, zachowaj wielkość liter podczas określania nazwy DNS urządzenia w regułach przenoszenia urządzeń i regułach automatycznego tagowania. Inaczej zasady nie będą działać.
- W kreatorze **Dodaj podrzędny Serwer administracyjny**, jeśli określisz konto z włączoną weryfikacją dwuetapową do uwierzytelniania na przyszłym Serwerze pomocniczym, kreator zakończy działanie z błędem. Aby rozwiązać ten problem, określ konto, dla którego weryfikacja dwuetapowa jest wyłączona, lub utwórz hierarchię z przyszłego serwera pomocniczego.
- Jeśli podczas logowania do Kaspersky Security Center Web Console, używasz uwierzytelniania domeny i określisz wirtualny Serwer administracyjny, z którym chcesz się połączyć, wylogujesz się, a następnie spróbujesz zalogować do głównego Serwera administracyjnego, Kaspersky Security Center Web Console połączy się do wirtualnego Serwera administracyjnego. Aby połączyć się z głównym Serwerem administracyjnym, ponownie otwórz przeglądarkę.
- Na liście zadań we właściwościach urządzenia może być wyświetlany nieprawidłowy stan zadania lokalnego.
- Szybkie/Pełne przeszukiwanie sieci Windows zwraca pusty wynik.
- Jeśli zainstalujesz Kaspersky Security Center Web Console z Identity and Access Manager, a następnie zmienisz Serwer administracyjny na Kaspersky Security Center Web Console, Identity and Access Manager nie otrzyma informacji o nowym Serwerze administracyjnym.
- Jeżeli otworzysz Kaspersky Security Center Web Console w różnych przeglądarkach i pobierzesz plik certyfikatu Serwera administracyjnego w oknie właściwości Serwera administracyjnego, pobrane pliki będą miały różne nazwy.
- Podczas próby przywrócenia obiektu z repozytorium **Kopia zapasowa** (**Operacje → Repozytoria → Kopia zapasowa**) lub wysłania obiektu do Kaspersky wystąpi błąd.
- Zarządzane urządzenie, które ma więcej niż jedną kartę sieciową, wysyła do Serwera administracyjnego informacje o adresie MAC karty sieciowej, która nie jest używana do łączenia się z Serwerem administracyjnym.
- Jeśli zainstalujesz Kaspersky Security Center Web Console z Identity and Access Manager, a następnie zmienisz Serwer administracyjny na Kaspersky Security Center Web Console, Identity and Access Manager nie otrzyma informacji o nowym Serwerze administracyjnym.