kaspersky

Kaspersky Security Center 14 Linux

© 2023 AO Kaspersky Lab

Spis treści

Grupa ról
HTTPS
Instalacja lokalna
Instalacja ręczna
Instalacja zdalna
JavaScript
Kaspersky Private Security Network (Private KSN)
Kaspersky Security Center Administrator
Kaspersky Security Center System Health Validator (SHV)
Kaspersky Security Center Web Server
Klient Serwera administracyjnego (urządzenie klienckie)
Konsola administracyjna
Kopia zapasowa danych Serwera administracyjnego
Macierzysty Serwer administracyjny
Niekompatybilna aplikacja
Ochrona antywirusowa sieci
Okres licencji
Operator Kaspersky Security Center
Pakiet instalacyjny
Plik klucza
Priorytet zdarzenia
Profil
Profil informacyjny
Profil konfiguracyjny
Przywracanie
Przywrócenie danych Serwera administracyjnego
Punkt dystrybucji
Repozytorium zdarzeń
Scentralizowane zarządzanie aplikacjami
Serwer administracyjny
Serwery aktualizacji Kaspersky
Sklep aplikacji
SSL
Stacja robocza administratora
Stan ochrony
Stan ochrony sieci
Strefa zdemilitaryzowana (DMZ)
Uprawnienia administracyjne
Ustawienia programu
Ustawienia zadania
Użytkownicy wewnętrzni
Wirtualny Serwer administracyjny
Właściciel urządzenia
Zadanie
Zadanie dla określonych urządzeń
Zadanie grupowe
Zadanie lokalne
Zarządzane urządzenia

System pomocy Kaspersky Security Center 14 Linux

	**Nowości** Zapoznaj się z nowościami w najnowszym wydaniu produktu.		**Aplikacje Kaspersky. Licencjonowanie i aktywacja** Aktywuj aplikacje Kaspersky w kilku krokach.
	**Wymagania sprzętowe i programowe** Sprawdź, które systemy operacyjne i wersje aplikacji są obsługiwane.		**Konfigurowanie ochrony sieci** Zarządzaj bezpieczeństwem organizacji.
	**Instalacja** Zainstaluj Serwer administracyjny i Kaspersky Security Center 14 Web Console.		**Aplikacje Kaspersky. Aktualizowanie baz danych i modułów aplikacji** Zachowaj niezawodność systemu ochrony.
	**Wykrywanie urządzeń w sieci** Wyszukuj istniejące i nowe urządzenia w sieci organizacji.		**Monitorowanie i raportowanie** Sprawdź swoją infrastrukturę, stany ochrony i statystyki.
	**Aplikacje Kaspersky. Zdalna instalacja** Zdalnie instaluj aplikacje Kaspersky.		**Dostosowanie punktów dystrybucji i/lub bram połączenia** Konfiguruj punkty dystrybucji.

Nowości

Kaspersky Security Center 14 Linux

Kaspersky Security Center 14 Linux posiada kilka nowych funkcji i ulepszeń:

- Oprócz zadania*Pobierz aktualizacje do repozytorium Serwera administracyjnego* antywirusowe bazy danych dla aplikacji zabezpieczających firmy Kaspersky można teraz pobierać za pomocą zadania *Pobierz aktualizacje do repozytoriów punktów dystrybucji*.

- Antywirusowe bazy danych i moduły aplikacji na zarządzanych urządzeniach mogą być propagowane i aktualizowane za pośrednictwem Serwera administracyjnego lub punktów dystrybucji. Możesz wybrać schemat aktualizacji optymalny dla Twojej organizacji, aby zmniejszyć obciążenie Serwera administracyjnego i zoptymalizować ruch danych w sieci firmowej.

- Kaspersky Security Center pobiera z serwerów aktualizacji Kaspersky tylko te aktualizacje, których żądają aplikacje zabezpieczające firmy Kaspersky. Zmniejsza to rozmiar pobieranych danych.

- Możesz teraz używać funkcji plików diff do pobierania antywirusowych baz danych i modułów oprogramowania. 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.

- Dodano zadanie *Weryfikacja aktualizacji*. Korzystając z tego zadania, możesz automatycznie sprawdzić pobrane aktualizacje pod kątem działania i błędów przed zainstalowaniem aktualizacji na zarządzanych urządzeniach.

Informacje o Kaspersky Security Center Linux

W tej sekcji można znaleźć informacje o przeznaczeniu Kaspersky Security Center Linux, jego głównych funkcjach i składnikach.

Kaspersky Security Center Linux (nazywany również Kaspersky Security Center) jest przeznaczony do wdrażania i zarządzania ochroną urządzeń z systemem Linux® przy użyciu Serwera administracyjnego opartego na systemie Linux, aby spełnić wymagania czystych środowisk Linux.

Kaspersky Security Center Linux umożliwia instalację aplikacji zabezpieczających firmy Kaspersky na urządzeniach w sieci firmowej, zdalne uruchamianie zadań skanowania i aktualizacji oraz zarządzanie politykami bezpieczeństwa zarządzanych aplikacji. Jako Administrator, możesz użyć szczegółowego pulpitu nawigacyjnego, który zawiera migawkę stanów urządzeń firmowych, szczegółowe raporty i szczegółowe ustawienia w zasadach ochrony.

W porównaniu z Kaspersky Security Center, które posiada Serwer administracyjny oparty na systemie Windows®, Kaspersky Security Center Linux ma inny zestaw funkcji.

Kaspersky Security Center Linux 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.
- Wykonywać zdalną instalację aplikacji Kaspersky i innych producentów oprogramowania.
- 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.
- 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.

Pakiet dystrybucyjny

Aplikację można kupić w sklepie internetowym Kaspersky (na przykład, https://www.kaspersky.com.pl/ lub u partnerów firmy.

Jeśli zakupisz Kaspersky Security Center Linux w sklepie internetowym, pobierz aplikację ze strony internetowej sklepu. Informacje potrzebne do aktywacji aplikacji są przesyłane drogą elektroniczną po dokonaniu płatności.

Wymagania sprzętowe i programowe

Serwer administracyjny

Minimalne wymagania sprzętowe:

- Procesor o częstotliwości taktowania 1 GHz lub większej. W przypadku 64-bitowych systemów operacyjnych minimalna częstotliwość taktowania procesora to 1.4 GHz.
- Pamięć RAM: 4 GB.
- Dostępne miejsce na dysku: 10 GB.

Obsługiwane są następujące systemy operacyjne:

- Debian GNU/Linux 11.x (Bullseye) 32-bitowy/64-bitowy
- Debian GNU/Linux 10.x (Buster) 32-bitowy/64-bitowy
- Debian GNU/Linux 9.x (Stretch) 32-bitowy/64-bitowy
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-bitowy
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64-bitowy
- CentOS 7.x 64-bitowy
- Red Hat Enterprise Linux Server 8.x 64-bitowy
- Red Hat Enterprise Linux Server 7.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
- Astra Linux Special Edition 1.7 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy) 64-bitowy
- Astra Linux Special Edition, wersja 1.6 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy) 64-bitowy
- Astra Linux Common Edition 2.12 64-bitowy
- Alt Server 10 64-bitowy
- Alt Server 9.2 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

- Oracle Linux 7 64-bitowy
- Oracle Linux 8 64-bitowy
- RED OS 7.3 Server 64-bitowy
- RED OS 7.3 Certified Edition 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
- Maszyna wirtualna oparta na jądrze. Obsługuje następujące systemy operacyjne:
  - Alt 8 SP Server (LKNV.11100-01) 64-bitowy
  - Alt Server 10 64-bitowy
  - Astra Linux Special Edition 1.7 (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 Server 64-bitowy
  - RED OS 7.3 Certified Edition 64-bitowy

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

- MySQL 5.7 Community 32-bitowy/64-bitowy
- MySQL 8.0 32-bitowy/64-bitowy
- MariaDB 10.5.x 32-bitowy/64-bitowy

- MariaDB 10.4.x 32-bitowy/64-bitowy
- MariaDB 10.3.22 i nowsze wersje 32-bitowe/64-bitowe
- MariaDB Server 10.3 32-bitowy/64-bitowy z silnikiem magazynowania InnoDB
- MariaDB 10.1.30 i nowsze wersje 32-bitowe/64-bitowe

Kaspersky Security Center 14 Web Console

Serwer Kaspersky Security Center 14 Web Console

Minimalne wymagania sprzętowe:

- Procesor: 4 rdzenie, częstotliwość taktowania wynosząca 2,5 GHz.
- Pamięć RAM: 8 GB.
- Dostępne miejsce na dysku: 40 GB.

Jeden z następujących systemów operacyjnych (tylko wersje 64-bitowe):

- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 9.x (Stretch)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12 (wszystkie pakiety Service Pack)
- SUSE Linux Enterprise Server 15 (wszystkie pakiety Service Pack)
- SUSE Linux Enterprise Desktop 15 (dodatek Service Pack) ARM 64-bitowy
- Astra Linux Special Edition 1.7 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy)
- Astra Linux Special Edition 1.6 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy)
- Astra Linux Common Edition 2.12
- Alt Server 10
- Alt Server 9.2

- Alt 8 SP Server (LKNV.11100-01)
- Alt 8 SP Server (LKNV.11100-02)
- Alt 8 SP Server (LKNV.11100-03)
- Oracle Linux 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition

Wśród platform wirtualizacji maszyna wirtualna oparta na jądrze jest obsługiwana w następujących systemach operacyjnych:

- Alt 8 SP Server (LKNV.11100-01) 64-bitowy
- Alt Server 10 64-bitowy
- Astra Linux Special Edition 1.7 (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 Server 64-bitowy
- RED OS 7.3 Certified Edition 64-bitowy

Urządzenia klienckie

W przypadku urządzenia klienckiego do korzystania z Kaspersky Security Center 14 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 14 Web Console.

Przeglądarki:

- Mozilla Firefox Extended Support Release w wersji 91.8.0 lub nowszej (91.8.0 wydano 5 kwietnia 2022 r.)
- Mozilla Firefox w wersji 99.0 lub nowszej (99.0 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

Agent sieciowy

Minimalne wymagania sprzętowe:

- Procesor o częstotliwości taktowania 1 GHz lub większej. W przypadku 64-bitowych systemów operacyjnych minimalna częstotliwość 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:

- Debian GNU/Linux 11.x (Bullseye) 32-bitowy/64-bitowy
- Debian GNU/Linux 10.x (Buster) 32-bitowy/64-bitowy
- Debian GNU/Linux 9.x (Stretch) 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 Server 18.04 LTS (Bionic Beaver) 32-bitowy/64-bitowy
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bitowy/64-bitowy
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bitowy/64-bitowy
- CentOS 8.x 64-bitowy
- CentOS 7.x 64-bitowy
- CentOS 7.x ARM 64-bitowy
- Red Hat Enterprise Linux Server 8.x 64-bitowy
- Red Hat Enterprise Linux Server 7.x 64-bitowy
- Red Hat Enterprise Linux Server 6.x 32-bitowy/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 (wszystkie dodatki Service Pack) ARM 64-bitowy
- openSUSE 15 64-bitowy
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64-bitowy

- Astra Linux Special Edition 1.7 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy) 64-bitowy
- Astra Linux Special Edition, wersja 1.6 (w tym tryb zamkniętego środowiska oprogramowania i tryb obowiązkowy) 64-bitowy
- Astra Linux Common Edition 2.12 64-bitowy
- Astra Linux Special Edition 4.7 ARM
- Alt Server 10 64-bitowy
- Alt Server 9.2 64-bitowy
- Alt Workstation 10 32-bitowy/64-bitowy
- Alt Workstation 9.2 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
- 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 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
- Lotos (rdzeń Linux w wersji 4.19.50, DE: MATE) 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
- Maszyna wirtualna oparta na jądrze. Obsługuje następujące systemy operacyjne:
  - Alt 8 SP Server (LKNV.11100-01) 64-bitowy
  - Alt Server 10 64-bitowy
  - Astra Linux Special Edition 1.7 (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

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

Informacje o Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console jest to aplikacja internetowa stworzona do zarządzania stanem systemu ochrony 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 14 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 14 Web Console przy użyciu swojej przeglądarki internetowej, przeglądarka nawiąże połączenie z serwerem Kaspersky Security Center 14 Web Console Server.

Kaspersky Security Center 14 Web Console działa w następujący sposób:

1. Użyj przeglądarki internetowej do nawiązania połączenia z Kaspersky Security Center 14 Web Console, gdzie wyświetlany jest interfejs portalu internetowego.
2. Użyj kontrolek portalu internetowego do wybrania polecenia, które chcesz uruchomić. Kaspersky Security Center 14 Web Console wykonuje następujące działania:
    - Jeśli wybrałeś polecenie używane do pobierania informacji (na przykład, do wyświetlania listy urządzeń), Kaspersky Security Center 14 Web Console wyśle do Serwera administracyjnego żądanie otrzymania informacji, pobierze wymagane dane, a następnie wyśle je do przeglądarki w przejrzystym formacie.
    - Jeśli wybrałeś polecenie używane do zarządzania (na przykład, do zdalnej instalacji aplikacji), Kaspersky Security Center 14 Web Console pobierze 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 14 Web Console to wielojęzykowa aplikacja. W każdej chwili możesz zmienić język interfejsu, bez ponownego otwierania aplikacji. Jeśli instalujesz Kaspersky Security Center 14 Web Console wraz z Kaspersky Security Center, Kaspersky Security Center 14 Web Console ma ten sam język interfejsu co plik instalacyjny. Jeśli instalujesz tylko Kaspersky Security Center 14 Web Console, aplikacja posiada ten sam język interfejsu co Twój system operacyjny. Jeśli Kaspersky Security Center 14 Web Console nie obsługuje języka pliku instalacyjnego lub systemu operacyjnego, język angielski jest ustawiony domyślnie.

Lista obsługiwanych aplikacji firmy Kaspersky

Kaspersky Security Center Linux obsługuje scentralizowane wdrażanie i zarządzanie Kaspersky Endpoint Security for Linux. Aplikacja ta pozwala chronić zarówno stacje robocze, jak i serwery plików. Zapoznaj się ze stroną internetową dotyczącą cyklu wsparcia technicznego produktów dla wersji aplikacji.

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.

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)
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	✓	✓

Podstawowe pojęcia

W tej sekcji wyjaśniono podstawowe pojęcia związane z Kaspersky Security Center Linux.

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 Kaspersky Security Center 14 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 14 Web Console zainstalowanej na urządzeniu z systemem Linux, aplikacja wyświetli nazwy Serwerów administracyjnych, które określiłeś jako zaufane w pliku odpowiedzi.

Możesz nawiązać połączenie z Serwerem administracyjnym poprzez Kaspersky Security Center 14 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.

W hierarchii Serwer administracyjny Kaspersky Security Center Linux może działać tylko jako dodatkowy serwer zarządzany przez podstawowy Serwer administracyjny Kaspersky Security Center oparty na systemie Windows lub Kaspersky Security Center Cloud Console.

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 konsolę Kaspersky Security Center 14 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 Linux 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 Linux uruchamia ponownie główny Serwer administracyjny i wszystkie wirtualne Serwery administracyjne.

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

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 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.

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 14 Linux"
- 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*. Możesz zainstalować Agenta sieciowego z jednego z następujących źródeł:

- 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.

Nazwy procesu uruchamianego przez Agenta sieciowego są następujące:

- klnagent64.service (dla 64-bitowego systemu operacyjnego)
- klnagent.service (dla 32-bitowego systemu operacyjnego)

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 z systemem Linux i zainstalowanym Agentem sieciowym. 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 będzie działało jako punkt dystrybucji oraz jako brama połączenia.

Urządzenie może być zarządzane tylko przez jeden Serwer administracyjny. Jeden Serwer administracyjny może obsługiwać maksymalnie 20 000 urządzeń.

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

Urządzenia, na których zainstalowany jest Kaspersky Security Center 14 Web Console Server, nazywane są *stacjami roboczymi administratora*. Administratorzy mogą używać tych urządzeń do scentralizowanego zdalnego zarządzania aplikacjami Kaspersky zainstalowanymi na urządzeniach klienckich.

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.

Sieciowa wtyczka administracyjna

Specjalny komponent—*sieciowa wtyczka zarządzająca*—jest używany do zdalnego zarządzania oprogramowaniem Kaspersky przy użyciu Kaspersky Security Center 14 Web Console. W dalszej części dokumentu webowa wtyczka zarządzająca jest zwana również *wtyczką zarządzającą*. Wtyczka zarządzająca to interfejs między Kaspersky Security Center 14 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 Kaspersky Customer Service.

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 14 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:

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.
- 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
- 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 zarówno przez administratora przy użyciu narzędzi Kaspersky Security Center 14 Web Console 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 Syslog oraz w dzienniku zdarzeń Kaspersky Security Center zarówno centralnie 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) 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 (patrz rysunek) 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.

Profil i lokalne ustawienia 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 rozsyłania uaktualnień, zdalnej instalacji aplikacji oraz gromadzenia 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 aktualizacji dla punktu dystrybucji.

  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 aplikacji firmy Kaspersky i innych producentów oprogramowania, w tym 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.

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.

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.

Agenci sieciowi z aktywnym profilem połączenia nie uczestniczą w wykrywaniu domen rozgłoszeniowych.

Kaspersky Security Center Linux 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. Adresy multicastowe IP, które zostały przydzielone w poprzednich wersjach aplikacji, nie zostaną zmienione.

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 Linux 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 we 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.

Licencjonowanie

Ta sekcja zawiera informacje dotyczące ogólnych zasad związanych z licencjonowaniem Kaspersky Security Center 14 Linux.

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 Linux i jego komponenty, na przykład, Agent sieciowy, ma swoją własną Umowę licencyjną.

Z warunkami Umowy Licencyjnej Użytkownika Końcowego dla Kaspersky Security Center Linux 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.

Z warunkami Umowy Licencyjnej Użytkownika Końcowego Agenta sieciowego dla systemu Linux można zapoznać się, korzystając z następujących metod:

- Podczas pobierania pakietu dystrybucyjnego Agenta sieciowego z serwerów sieciowych Kaspersky.
- Podczas instalacji Agenta sieciowego dla systemu Linux.

  Należy pamiętać, że podczas instalacji Agenta sieciowego dla systemu Linux Umowa licencyjna użytkownika końcowego dla Agenta sieciowego jest wyświetlana w języku angielskim. Możesz sprawdzić Umowę licencyjną użytkownika końcowego dla Agenta sieciowego w innych językach w folderze /opt/kaspersky/klnagent64/share/license przed zaakceptowaniem warunków Umowy licencyjnej użytkownika końcowego podczas instalacji.

- Czytając dokument license.txt dołączony do pakietu dystrybucyjnego Agenta sieciowego dla systemu Linux.
- Czytając dokument license.txt w folderze instalacyjnym Agenta sieciowego dla systemu Linux.

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 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:

- *Testowa* – 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 Linux zostają wyłączone. Aby kontynuować korzystanie z aplikacji, należy zakupić licencję komercyjną.

  Możesz aktywować aplikację licencją testową tylko raz.

- *Komercyjna* – płatna licencja oferowana podczas zakupu aplikacji.

  Po wygaśnięciu licencji komercyjnej aplikacja nadal działa, ale z ograniczoną funkcjonalnością (na przykład, uaktualnienia baz danych Kaspersky Security Center są niedostępne). Aby kontynuować korzystanie ze wszystkich funkcji Kaspersky Security Center, musisz odnowić swoją licencję komercyjną.

Zalecamy odnowienie licencji przed jej wygaśnięciem, aby zapewnić maksymalną ochronę przed wszystkimi zagrożeniami.

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.

Przeglądanie Polityki prywatności

Polityka prywatności jest dostępna online pod adresem https://www.kaspersky.com/products-and-services-privacy-policy.

Polityka Prywatności dostępna jest również w trybie offline:

- Możesz przeczytać Politykę prywatności przed zainstalowaniem Kaspersky Security Center.
- Tekst Polityki prywatności znajduje się w pliku license.txt w folderze instalacyjnym Kaspersky Security Center.
- Plik privacy_policy.txt jest dostępny na zarządzanym urządzeniu w folderze instalacyjnym Agenta sieciowego.
- Możesz rozpakować plik privacy_policy.txt z pakietu dystrybucyjnego Agenta sieciowego.

Opcje licencjonowania Kaspersky Security Center

Kaspersky Security Center jest dostarczany jako część aplikacji Kaspersky do ochrony sieci korporacyjnych. Można ją również pobrać ze strony firmy Kaspersky.

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.
- 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.

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 przekazywaniu danych

Dane przekazywane Posiadaczowi praw

Udostępnione w Umowie licencyjnej użytkownika końcowego systemu Kaspersky Security Center 14 Linux.

Dane przetwarzane lokalnie

Kaspersky Security Center Linux służy do scentralizowanego wykonywania podstawowych zadań dotyczących administracji i zarządzania w sieci firmy. Kaspersky Security Center Linux zapewnia administratorowi dostęp do szczegółowych informacji dotyczących poziomu ochrony sieci organizacji; Kaspersky Security Center Linux umożliwia administratorowi skonfigurowanie wszystkich składników ochrony opartych o aplikacje Kaspersky. Kaspersky Security Center Linux 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
- 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 Linux mógł wykonywać główne funkcje, może otrzymywać, przechowywać i przetwarzać następujące informacje:

- Informacje o urządzeniach w sieci organizacji otrzymane w wyniku wykrywania urządzeń w sieci lub poprzez skanowanie interwałów IP. Serwer administracyjny gromadzi dane 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 Kaspersky Security Center 14 Web Console:
  - Specyfikacje techniczne zarządzanego urządzenia i jego komponenty wymagane do identyfikacji urządzenia: wyświetlana nazwa i opis urządzenia, 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 komponentów wymagane do audytu zarządzanych urządzeń: architektura systemu operacyjnego, dostawca systemu operacyjnego, numer kompilacji systemu operacyjnego, identyfikator wersji systemu operacyjnego, folder lokalizacji systemu operacyjnego, jeśli urządzenie jest maszyną wirtualną — typ maszyny wirtualnej.
  - 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 Kaspersky Security Center 14 Web Console.
- 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, 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.

- Dane znajdujące się w zdarzeniach z komponentów Kaspersky Security Center Linux i zarządzanych aplikacji firmy Kaspersky. Agent sieciowy przesyła dane z urządzenia na Serwer administracyjny.
- Ustawienia komponentów Kaspersky Security Center Linux i zarządzanych aplikacji firmy Kaspersky, przedstawionych w zasadach i profilach zasad. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.
- Ustawienia zadania komponentów Kaspersky Security Center Linux i zarządzanych aplikacji firmy Kaspersky. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.
- Dane przetwarzane przez funkcję Zarządzanie lukami i poprawkami. Agent sieciowy przesyła z urządzenia do Serwera administracyjnego informacje o sprzęcie wykrytym na zarządzanych urządzeniach (Rejestr sprzętu).
- Kategorie użytkownika dla aplikacji. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.
- Szczegóły plików wykonywalnych wykrytych na zarządzanych urządzeniach przez funkcję Kontroli aplikacji. 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 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 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.
- 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.
- Szczegóły wprowadzonych kodów aktywacyjnych. Użytkownik wprowadza dane w Konsoli administracyjnej lub w interfejsie konsoli Kaspersky Security Center 14 Web Console.
- Konta użytkowników: nazwa, opis, imię i nazwisko, adres e-mail, główny numer telefonu i hasło. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.
- Historia rewizji zarządzanych obiektów. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.

- Rejestr usuniętych zarządzanych obiektów. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.

- Pakiety instalacyjne utworzone z pliku, a także ustawienia instalacji. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.

- Dane wymagane do wyświetlania ogłoszeń z Kaspersky w Kaspersky Security Center 14 Web Console. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.

- Dane wymagane do działania wtyczek zarządzanych aplikacji w konsoli Kaspersky Security Center 14 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 14 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 14 Web Console.

- Dziennik zdarzeń aplikacji Kaspersky dla komponentów Kaspersky Security Center Linux 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 Linux. Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.

- Wszelkie dane Serwera administracyjnego, jakie Użytkownik wprowadza w konsoli Kaspersky Security Center 14 Web Console.

- Wszelkie dane, jakie Użytkownik wprowadza w interfejsie konsoli Kaspersky Security Center 14 Web Console.

Dane wymienione powyżej mogą zostać przedstawione w Kaspersky Security Center Linux, jeśli stosowana jest jedna z następujących metod:

- Użytkownik wprowadza dane w interfejsie konsoli Kaspersky Security Center 14 Web Console.

- 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.

Wymienione dane są przechowywane w bazie danych Serwera administracyjnego. Nazwy użytkowników i hasła są przechowywane w postaci zaszyfrowanej.

Wszystkie przetworzone lokalnie dane mogą być przesyłane do Kaspersky tylko poprzez pliki zrzutów, pliki śledzenia lub pliki raportów komponentów Kaspersky Security Center Linux, w tym pliki raportów utworzone przez instalatory i narzędzia.

Firma Kaspersky chroni wszelkie zebrane informacje zgodnie z prawem oraz obowiązującymi przepisami stosowanymi w firmie Kaspersky. Dane są przesyłane za pośrednictwem bezpiecznego kanału.

Klikając odnośniki w Konsoli administracyjnej lub konsoli Kaspersky Security Center 14 Web Console, Użytkownik wyraża zgodę na automatyczne przesyłanie następujących danych:

- Kod Kaspersky Security Center Linux
- Wersja Kaspersky Security Center Linux
- Lokalizacja Kaspersky Security Center Linux
- 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.

Informacje o subskrypcji

Subskrypcja na Kaspersky Security Center Linux jest to zamówienie aplikacji z wybranymi ustawieniami (data wygaśnięcia subskrypcji, liczba chronionych urządzeń). Możesz zarejestrować swoją subskrypcję na Kaspersky Security Center Linux 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 Linux z subskrypcją, należy wprowadzić kod aktywacyjny otrzymany od dostawcy usługi.

Możesz zastosować dla Kaspersky Security Center Linux 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 Linux automatycznie próbuje uzyskać dostęp do serwera aktywacji w określonych przedziałach czasu, aż do wygaśnięcia subskrypcji. Możesz odnowić swoją subskrypcję na stronie dostawcy usługi.

Zdarzenia przekroczenia ograniczeń licencyjnych

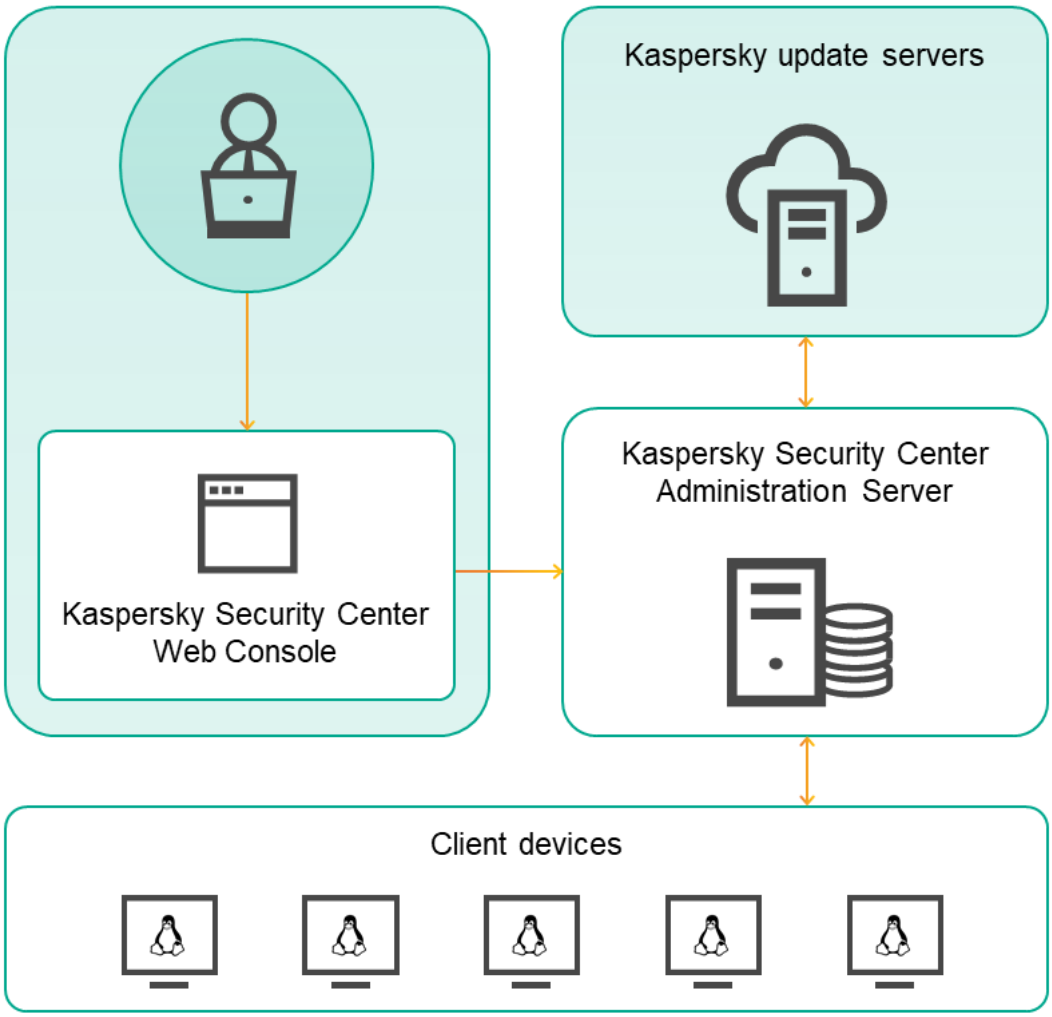
Kaspersky Security Center Linux pozwala uzyskać informacje o zdarzeniach, gdy pewne ograniczenia licencyjne zostaną przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich.

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**.

Architektura

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



Architektura Kaspersky Security Center 14 Linux

Kaspersky Security Center 14 Linux zawiera następujące główne składniki:

- **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 14 Linux. Każde urządzenie, które musi być chronione, musi posiadać zainstalowaną jedną z aplikacji zabezpieczających Kaspersky.

Diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center 14 Web Console

Rysunek poniżej przedstawia diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center 14 Web Console.

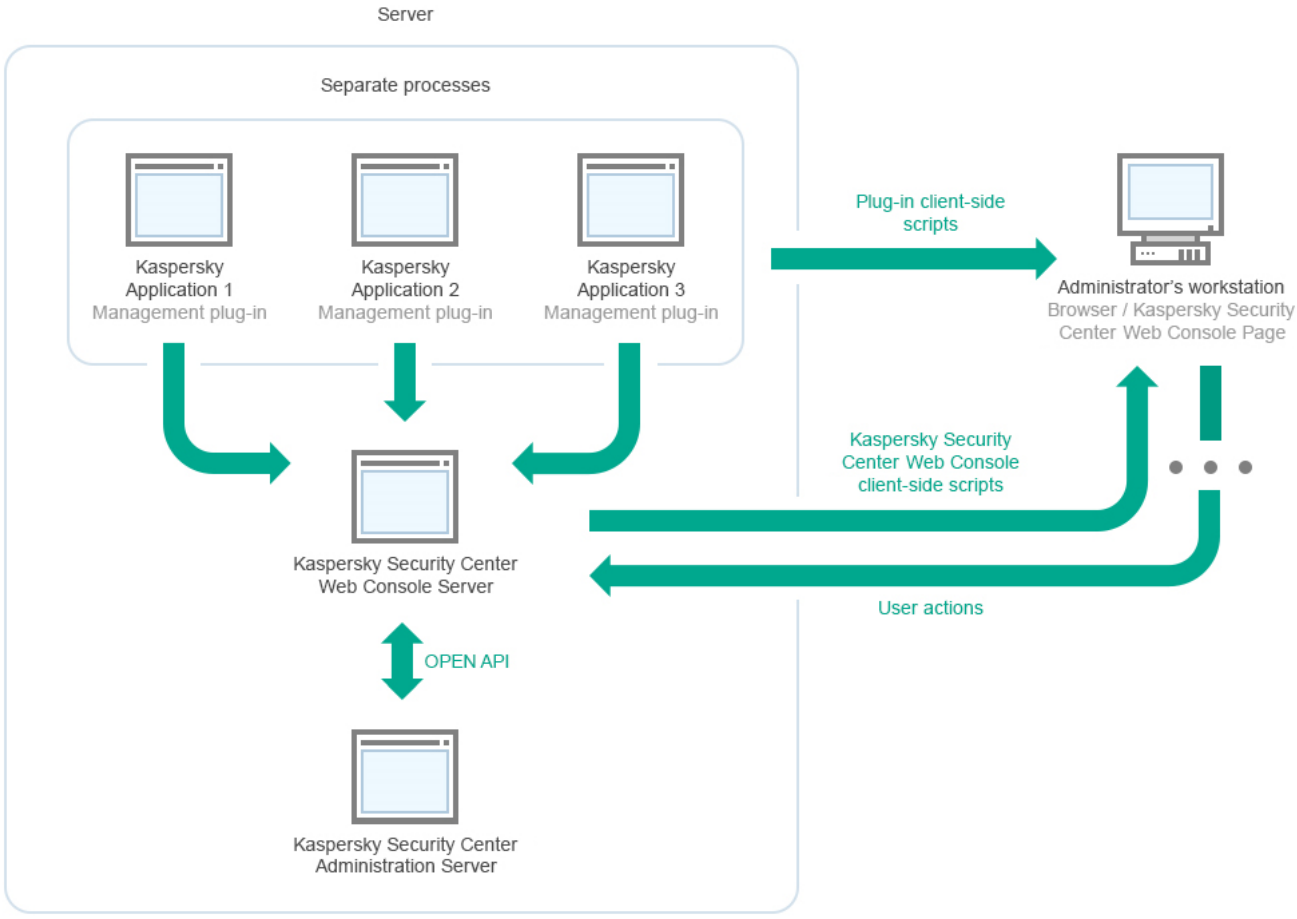


Diagram zdalnej instalacji Serwera administracyjnego Kaspersky Security Center i konsoli Kaspersky Security Center 14 Web Console

Wtyczki zarządzające dla aplikacji Kaspersky zainstalowanych na chronionych urządzeniach (jedna wtyczka dla każdej aplikacji) są instalowane wraz z serwerem konsoli Kaspersky Security Center 14 Web Console.

Jako administrator uzyskujesz dostęp do Kaspersky Security Center 14 Web Console przy użyciu przeglądarki na swojej stacji roboczej.

Jeśli wykonujesz określone działania w Kaspersky Security Center 14 Web Console, serwer Kaspersky Security Center 14 Web Console Server komunikuje się z serwerem administracyjnym Kaspersky Security Center poprzez interfejs OpenAPI. Serwer Kaspersky Security Center 14 Web Console Server żąda wymaganych informacji z serwera administracyjnego Kaspersky Security Center i wyświetla wyniki Twoich działań w Kaspersky Security Center 14 Web Console.

Porty używane przez Kaspersky Security Center Linux

Poniżej znajduje się tabela zawierająca domyślne porty, które muszą być otwarte na Serwerze administracyjnym i urządzeniach klienckich. Jeśli chcesz, możesz zmienić każdy z tych domyślnych numerów portów.

Porty używane przez Serwer administracyjny Kaspersky Security Center Linux

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 numer domyślnego portu w Sekcji **Serwer WWW** w oknie właściwości Serwera administracyjnego.
8061	klcsweb	TCP (TLS)	Przesyłanie opublikowanych pakietów instalacyjnych na urządzenia klienckie	Publikowanie pakietów instalacyjnych. Możesz zmienić numer domyślnego portu w Sekcji **Serwer WWW** w oknie właściwości Serwera administracyjnego.
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 podczas instalacji Kaspersky Security Center Linux; możesz zmienić numer domyślnego portu do odbierania połączeń z podrzędnych Serwerów administracyjnych podczas tworzenia hierarchii Serwerów administracyjnych.
13000	klserver	UDP	Pobieranie informacji o urządzeniach, które zostały wyłączone, z Agentów sieciowych	Zarządzanie urządzeniami klienckimi. Możesz zmienić domyślny numer portu w ustawieniach profilu Agenta sieciowego.
13299	klserver	TCP (TLS)	Odbieranie połączeń od Kaspersky Security Center 14 Web Console do Serwera administracyjnego; odbieranie połączeń do Serwera administracyjnego poprzez OpenAPI	Kaspersky Security Center 14 Web Console, OpenAPI. Domyślny numer portu można zmienić w oknie właściwości Serwera administracyjnego (w podsekcji **Porty połączeń** w sekcji **Ogólne**) lub podczas tworzenia hierarchii Serwerów administracyjnych.
14000	klserver	TCP	Odbieranie połączeń od Agentów sieciowych	Zarządzanie urządzeniami klienckimi.

				Możesz zmienić numer domyślnego portu podczas konfigurowania portów połączeń podczas instalacji Kaspersky Security Center Linux 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 usługa KSN Proxy jest uruchomiona na urządzeniu)	ksnproxy	UDP	Odbieranie żądań od zarządzanych urządzeń do serwera KSN proxy	Serwer KSN proxy. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego.
17000	klactprx	TCP (TLS)	Odbieranie połączeń dla aktywacji aplikacji od zarządzanych urządzeń	Aktywacja przy użyciu serwera proxy dla zarządzanych urządzeń. Możesz zmienić numer domyślnego portu w oknie właściwości Serwera administracyjnego (w podsekcji **Dodatkowe porty** sekcji **Ogólne**).
19170	klserver	HTTPS (TLS)	Tunelowanie połączeń z zarządzanymi urządzeniami przy użyciu narzędzia klsctunnel	Zdalne nawiązywanie połączenia z zarządzanymi urządzeniami przy użyciu Kaspersky Security Center 14 Web Console. Domyślny numer portu można zmienić za pomocą narzędzia klscflag.

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 MariaDB Server). Odpowiednie informacje można znaleźć w dokumentacji do DBMS.

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

Port używany przez Kaspersky Security Center Linux Web Console Server

Numer portu	Nazwa procesu, który otwiera port	Protokół	Przeznaczenie portu	Obszar
8080	Node.js: Server-side JavaScript	TCP (TLS)	Odbieranie połączeń z przeglądarki do Kaspersky	Kaspersky Security Center 14 Web Console.

			Security Center 14 Web Console	Podczas instalacji Kaspersky Security Center 14 Web Console możesz zmienić domyślny numer portu. Jeśli instalujesz konsolę Kaspersky Security Center 14 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 domyślny numer portu w ustawieniach profilu Agenta sieciowego.
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 Serwera administracyjnego.

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 we właściwościach punktu dystrybucji.
13111 (tylko wtedy, gdy usługa KSN Proxy jest	ksnproxy	TCP	Odbieranie żądań od zarządzanych	Serwer KSN proxy.

uruchomiona na urządzeniu)			urządzeń do serwera KSN proxy	Możesz zmienić numer domyślnego portu we właściwościach punktu dystrybucji.
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 we właściwościach punktu dystrybucji.

Porty używane przez Kaspersky Security Center 14 Web Console

Tabela poniżej wyświetla porty, które muszą być otwarte na urządzeniu, na którym jest zainstalowany Kaspersky Security Center 14 Web Console Server (zwany również Kaspersky Security Center 14 Web Console).

Porty używane przez Kaspersky Security Center 14 Web Console

Numer portu	Nazwa usługi	Protokół	Przeznaczenie portu	Obsz
2001	Wtyczka KSCWebConsolePlugin	HTTPS	Port API używany przez procesy wtyczki zarządzania do odbierania żądań z KSCWebConsoleManagementService	Uruchami procesów node.exe wtyczek zarządzar
1329, 2003	KSCWebConsoleManagementService	HTTPS	Port API, który jest używany do otrzymywania żądań z usługi KSCWebConsole działającej na tym samym urządzeniu	Aktualizo kompone Kaspersk Security Center 14 Console
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 Center 14 Console
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 Center 14 Console i aktualizov składnikó Kaspersk Security Center 14 Console
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	Porty API brokera komunikatów, które są używane do komunikacji między procesami Kaspersky Security Center 14 Web Console oraz wtyczek administracyjnych	Interakcja programu Kaspersk Security Center 14 Console i wtyczek zarządzaj

Instalacja

Ta sekcja opisuje instalację Kaspersky Security Center i Kaspersky Security Center 14 Web Console.

Główny scenariusz instalacji

Zgodnie ze scenariuszem, możesz przeprowadzić instalację Serwera administracyjnego Kaspersky Security Center 14 i konsoli Kaspersky Security Center 14 Web Console, przeprowadzić wstępną konfigurację Serwera administracyjnego przy użyciu Kreatora wstępnej konfiguracji, a także instalację aplikacji firmy Kaspersky na zarządzanych urządzeniach przy użyciu Kreatora wdrażania ochrony.

Wymagania wstępne

Musisz posiadać klucz licencyjny (kod aktywacyjny) do Kaspersky Endpoint Security for Buisness lub klucze licencyjne (kody aktywacyjne) do aplikacji zabezpieczających Kaspersky.

Jeśli najpierw chcesz wypróbować Kaspersky Security Center 14 Linux, możesz uzyskać bezpłatną, 30-dniową wersję testową na stronie internetowej Kaspersky.

Etapy

Główny scenariusz instalacji przebiega etapami:

1. **Wybieranie struktury ochrony organizacji**

   Zapoznaj się ze szczegółowymi informacjami dotyczącymi komponentów Kaspersky Security Center Linux. 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).

   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.

2. **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.

3. **Instalowanie systemu zarządzania bazą danych (DBMS)**

   Zainstaluj system DBMS, który będzie używany przez Kaspersky Security Center lub użyj istniejącego systemu.

4. **Konfigurowanie portów**

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

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

5. **Instalowanie Kaspersky Security Center**

Wybierz urządzenie z systemem Linux, którego chcesz używać jako Serwera administracyjnego, upewnij się, że spełnia ono wymagania sprzętowe i programowe, a następnie zainstaluj na nim Kaspersky Security Center. Wersja serwerowa Agenta sieciowego zostanie automatycznie zainstalowana na urządzeniu wraz z Serwerem administracyjnym.

6. **Instalacja programu Kaspersky Security Center 14 Web Console i wtyczek zarządzających**

   Wybierz urządzenie Linux, którego zamierzasz używać jako stację roboczą administratora, upewnij się, że spełnia ono wymagania programowe i sprzętowe, a następnie zainstaluj na nim Kaspersky Security Center 14 Web Console. Możesz zainstalować Kaspersky Security Center 14 Web Console również na tym samym urządzeniu, na którym jest zainstalowany Serwer administracyjny, lub na innym.

   Pobierz wtyczkę internetową do zarządzania Kaspersky Endpoint Security for Linux a następnie zainstaluj go na tym samym urządzeniu, na którym zainstalowano Kaspersky Security Center 14 Web Console.

7. **Instalowanie Kaspersky Endpoint Security for Linux i Agenta sieciowego na urządzeniu Serwera administracyjnego**

   Domyślnie aplikacja nie traktuje urządzenia Serwera administracyjnego jako urządzenia zarządzanego. Aby chronić Serwer administracyjny przed wirusami i innymi zagrożeniami oraz zarządzać urządzeniem jak każdym innym zarządzanym urządzeniem, zalecamy zainstalowanie Kaspersky Endpoint Security for Linux i Agenta sieciowego dla systemu Linux na urządzeniu Serwera administracyjnego. W takim przypadku Agent sieciowy dla systemu Linux jest instalowany i działa niezależnie od wersji serwerowej Agenta sieciowego zainstalowanego wraz z Serwerem administracyjnym.

8. **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.

9. **Wyszukiwanie urządzeń w sieci**

   Odkryj urządzenia ręcznie. Kaspersky Security Center Linux pobiera adresy i nazwy wszystkich urządzeń wykrytych w sieci. Następnie możesz użyć Kaspersky Security Center Linux do zainstalowania aplikacji firmy Kaspersky i oprogramowania innych producentów na wykrytych urządzeniach. Kaspersky Security Center Linux regularnie uruchamia wyszukiwanie urządzeń, co oznacza, że jeśli nowe instancje pojawią się w sieci, zostaną wykryte automatycznie.

10. **Rozmieszczanie urządzeń w grupach administracyjnych**

    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.

11. **Przypisywanie punktów dystrybucji**

    Punkty dystrybucji są przydzielane do grup administracyjnych automatycznie, ale możesz też przydzielić 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.

12. **Instalowanie Agenta sieciowego i aplikacji zabezpieczających na urządzeniach w sieci**

    Wdrożenie ochrony w sieci firmowej obejmuje instalację Agenta sieciowego i aplikacji zabezpieczających na urządzeniach, które zostały wykryte przez Serwer administracyjny podczas wykrywania urządzenia.

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).

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

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

14. **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.

15. **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.

Instalowanie systemu zarządzania bazą danych

Zainstaluj system zarządzania bazą danych (DBMS), który będzie używany przez Kaspersky Security Center. Możesz wybrać jeden z obsługiwanych DBMS.

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

Jeśli korzystasz z MariaDB, musisz skonfigurować zalecane ustawienia w celu optymalnej pracy DBMS z Kaspersky Security Center.

Konfigurowanie serwera MariaDB x64 do pracy z Kaspersky Security Center 14 Linux

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.cnf

W celu skonfigurowania pliku my.cnf:

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

2. Wprowadź następujące wiersze do pliku my.cnf:

```
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.

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`, `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. Upewnij się, że 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 wartości `on`, to dodatki optymalizujące są włączone.

   Jeśli tych wierszy brakuje lub mają one wartości `off`, musisz wykonać następujące czynności:

   a. Otwórz plik my.cnf w dowolnym edytorze tekstu.

   b. Dodaj do pliku my.cnf następujące wiersze:

   ```
   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.

Instalowanie Kaspersky Security Center

Ta procedura opisuje sposób instalacji Kaspersky Security Center.

Przed instalacją:

- Instalowanie systemu zarządzania bazą danych.
- Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center, działa jedna z obsługiwanych dystrybucji systemu Linux.

Użyj pliku instalacyjnego — ksc64_[version_number]_amd64.deb lub ksc64-[version_number].x86_64.rpm — który odpowiada dystrybucji Linux zainstalowanej na urządzeniu. Plik instalacyjny można pobrać ze strony internetowej Kaspersky.

W celu zainstalowania Kaspersky Security Center:

1. W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

2. Utwórz grupę „kladmins" i konto nieuprzywilejowane „ksc". Konto musi należeć do grupy „kladmins". Aby to zrobić, kolejno uruchom następujące polecenia:
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

3. Uruchom instalację Kaspersky Security Center. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

   - `# apt install /<path>/ksc64_[ version_number ]_amd64.deb`

   - `# yum install /<path>/ksc64-[ version_number ].x86_64.rpm -y`

4. Uruchom konfigurację Kaspersky Security Center:
   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Przeczytaj Umowę Licencyjną Użytkownika Końcowego (EULA) i Politykę prywatności. Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź następujące wartości:

   a. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki umowy licencyjnej. Wpisz `n`, jeśli nie akceptujesz warunków umowy licencyjnej. Aby korzystać z Kaspersky Security Center, musisz zaakceptować warunki umowy licencyjnej.

   b. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Polityki Prywatności oraz zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności. Wpisz `n`, jeśli nie akceptujesz warunków Polityki Prywatności. Aby korzystać z Kaspersky Security Center, musisz zaakceptować warunki Polityki prywatności.

6. Po wyświetleniu monitu wprowadź następujące ustawienia:

   a. Wprowadź nazwę DNS Serwera administracyjnego lub statyczny adres IP.

   b. Wprowadź numer portu Serwera administracyjnego. Domyślnie wykorzystywany jest port 14000.

   c. Wprowadź numer portu SSL Serwera administracyjnego. Domyślnie wykorzystywany jest port 13000.

   d. Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać:

      - Jeśli masz od 1 do 100 urządzeń sieciowych, wpisz 1.

      - Jeśli masz od 101 do 1000 urządzeń sieciowych, wpisz 2.

      - Jeśli masz więcej niż 1000 urządzeń sieciowych, wpisz 3.

   e. Wprowadź nazwę grupy zabezpieczeń dla usług. Domyślnie używana jest grupa „kladmins".

f. Wprowadź nazwę konta, aby uruchomić usługę Serwera administracyjnego. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „ksc".

g. Wprowadź nazwę konta, aby uruchomić inne usługi. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „ksc".

h. Wprowadź adres IP urządzenia, na którym zainstalowana jest baza danych.

i. Wprowadź numer portu bazy danych. Ten port jest używany do komunikacji z Serwerem administracyjnym. Domyślnie wykorzystywany jest port 3306.

j. Wprowadź nazwę bazy danych.

k. Wprowadź login konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

l. Wprowadź hasło konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

Poczekaj, aż usługi zostaną dodane i uruchomione automatycznie:

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. Utwórz konto, które będzie działać jako administrator Serwera administracyjnego. Wprowadź nazwę użytkownika i hasło.

Hasło musi być zgodne z następującymi regułami:

- Hasło użytkownika nie może mieć mniej niż 8 ani więcej niż 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Użytkownik zostanie dodany i zainstalowany Kaspersky Security Center.

Weryfikacja usługi

Użyj następujących poleceń, aby sprawdzić, czy usługa jest uruchomiona:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`

- `# systemctl status klwebsrv_srv.service`

Instalowanie Kaspersky Security Center 14 Web Console

Ta sekcja opisuje sposób oddzielnego zainstalowania serwera Kaspersky Security Center 14 Web Console Server (zwany również Kaspersky Security Center 14 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 14 Web Console:

1. Upewnij się, że urządzenie, na którym chcesz zainstalować Kaspersky Security Center 14 Web Console, jest uruchomione na jednej z obsługiwanych dystrybucji systemu Linux.
2. Przeczytaj umowę licencyjną użytkownika końcowego (EULA) w pakiecie instalacyjnym (plik /var/opt/kaspersky/ksc-web-console/license-<XX>.txt, gdzie <XX> to kod języka). Jeśli nie akceptujesz warunków Umowy licencyjnej, nie instaluj aplikacji.
3. Utwórz plik odpowiedzi, który zawiera parametry połączenia Kaspersky Security Center 14 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 14 Web Console w systemie operacyjnym Linux ALT, musisz określić numer portu inny niż 8080, ponieważ port 8080 jest używany przez system operacyjny.

   Konsola Kaspersky Security Center 14 Web Console nie może zostać zaktualizowana 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 zaktualizowania Kaspersky Security Center 14 Web Console z pliku .deb, uruchom następujące polecenie:
     ```
     $ sudo dpkg -i ksc-web-console-[build_number].x86_64.deb
     ```
   - W celu zainstalowania Kaspersky Security Center 14 Web Console z pliku .rpm uruchom jedno z następujących poleceń:
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[build_number].x86_64.rpm
     ```
     lub
     ```
     $ sudo alien -i 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. Konsola Kaspersky Security Center 14 Web Console jest instalowana w następującym katalogu: /var/opt/kaspersky/ksc-web-console.

5. Uruchom ponownie wszystkie usługi Kaspersky Security Center 14 Web Console, uruchamiając następujące polecenie:
   ```
   $ sudo systemctl restart KSC*
   ```

Po zakończeniu instalacji, możesz użyć swojej przeglądarki internetowej do otwarcia i zalogowania się w konsoli Kaspersky Security Center 14 Web Console.

Parametry instalacji Kaspersky Security Center 14 Web Console

Aby zainstalować Kaspersky Security Center 14 Web Console Server na urządzeniach działających pod kontrolą systemu Linux, musisz utworzyć plik odpowiedzi — plik .json, który zawiera parametry połączenia Kaspersky Security Center 14 Web Console z Serwerem administracyjnym.

Poniżej znajduje się 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 14 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 14 Web Console na urządzeniach działających pod kontrolą systemu Linux

Parametr	Opis	Dostępne war
`adres`	Adres Kaspersky Security Center 14 Web Console Server (wymagane).	Wartość wiersza.
`port`	Numer portu, którego Kaspersky Security Center 14 Web Console Server użyje do nawiązywania połączenia z Serwerem administracyjnym (wymagane).	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 jest

`enableLog`	Czy włączyć rejestrowania aktywności Kaspersky Security Center 14 Web Console.	Wartość zerojedynkowa: • `true`—rejestrowanie jest włączone (w • `false`—rejestrowanie jest wyłączone

`zaufane`	Lista zaufanych Serwerów administracyjnych upoważnionych do nawiązywania połączenia z Kaspersky Security Center 14 Web Console. Każdy Serwer administracyjny musi być zdefiniowany z następującymi parametrami:
	• Adres Serwera administracyjnego
	• Port OpenAPI, który jest używany przez Kaspersky Security Center 14 Web Console do nawiązywania połączenia z 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.
		Wartość wiersza w następującym formac
		`" server address|port|certificate`
		Na przykład:
		`"X.X.X.X|13299|/cert/server-1.ce`
		`1||Y.Y.Y.Y|13299|/cert/server-2.`

`acceptEula`	Czy chcesz zaakceptować warunki Umowy licencyjnej (EULA). Plik zawierający warunki Umowy licencyjnej jest pobierany wraz z plikiem instalacyjnym.	Wartość zerojedynkowa: • `true`—W pełni przeczytałem, zrozumi Umowy licencyjnej. • `false`—Nie akceptuję postanowień i (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_srv do korzystania z istniejącego certyfikatu. niestandardowego określ ścieżkę, w które 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 formac name". Przykład: „Grupa1:Użytkownik1”. Jeśli nie określono żadnej wartości, instala Center 14 Web Console utworzy nowe ko user_management_%uid% .
managementServiceAccount	Nazwa konta uprzywilejowanego, w ramach którego uruchomiona jest usługa KSCWebConsoleManagement.	Wartość wiersza w następującym formac name". Przykład: „Grupa1:Użytkownik1”. Jeśli nie określono żadnej wartości, instala Center 14 Web Console utworzy nowe ko user_nodejs_%uid%.
serviceWebConsoleAccount	Nazwa konta, w ramach którego uruchomiona jest usługa KSCSvcWebConsole .	Wartość wiersza w następującym formac name". Przykład: „Grupa1:Użytkownik1”. Jeśli nie określono żadnej wartości, instala Center 14 Web Console utworzy nowe ko user_svc_nodejs_%uid% .
pluginAccount	Nazwa konta, pod którym uruchomiona jest usługa KSCWebConsolePlugin.	Wartość wiersza w następującym formac name". Przykład: „Grupa1:Użytkownik1”. Jeśli nie określono żadnej wartości, instala Center 14 Web Console utworzy nowe ko user_web_plugin_%uid%.
messageQueueAccount	Nazwa konta, pod którym uruchomiona jest usługa KSCWebConsoleMessageQueue.	Wartość wiersza w następującym formac name". Przykład: „Grupa1:Użytkownik1”. Jeśli nie określono żadnej wartości, instala Center 14 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 14 Web Console utworzy domyślną grupę bezpieczeństwa, a następnie utworzy w tej grupie konta użytkowników o domyślnych nazwach.

Konta do pracy z DBMS

Poniższa tabela zawiera informacje o właściwościach kont wybranych do pracy z MariaDB DBMS.

Lokalny system DBMS to system DBMS zainstalowany na tym samym urządzeniu co Serwer administracyjny. *Zdalny system DBMS* to system DBMS zainstalowany na innym urządzeniu.

Należy przydzielić wszystkie wymagane uprawnienia dla konta Serwera administracyjnego przed uruchomieniem usługi Serwera administracyjnego.

DBMS: MariaDB

Lokalizacja DBMS	Lokalny lub zdalny.	Lokalny lub zdalny.
Kto utworzył bazę danych KAV	Instalator (automatycznie).	Administrator (ręcznie).
Konto, z poziomu którego uruchomiony jest instalator	Lokalny lub domenowy, z uprawnieniami administratora lokalnego.	Lokalny lub domenowy, z uprawnieniami administratora lokalnego.
Konto usługi Serwera administracyjnego	Lokalne lub domeny.	Lokalne lub domeny.
Uprawnienia wewnętrznego konta DBMS używanego przez instalatora i usługę Serwera administracyjnego w celu uzyskania dostępu do DBMS	Wymagany jest dostęp do roota.	`GRANT ALL` dla bazy danych KAV i `SELECT` , `SHOW VIEW` , `PROCESS` dla tabel systemowych.

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.

Wdrożenie aplikacji firmy Kaspersky odbywa się w krokach:

1. **Tworzenie konta dla usług Kaspersky Security Center**

   Utwórz nowe lub wybierz istniejące konto użytkownika domeny, na którym będą uruchamiane usługi Kaspersky Security Center. Dodaj wybrane konto w grupie administratorów lokalnych na każdym z węzłów i na serwerze plików.

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)**

   Masz dwie opcje:

   - Jeśli chcesz korzystać z MariaBD Galera Cluster, nie potrzebujesz dedykowanego komputera dla DBMS. Zainstaluj klaster MariaDB Galera Cluster na każdym z węzłów.
   - Jeśli chcesz użyć innego obsługiwanego DBMS, zainstaluj wybrany 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.

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.

W klastrze pracy awaryjnej Kaspersky, wszystkie usługi Kaspersky Security Center są zarządzane automatycznie. Nie próbuj ponownie uruchamiać usług ręcznie.

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 z systemem Linux z systemem plików EXT4. 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). Jeśli używasz MariaBD Galera Cluster jako DBMS, dedykowany komputer do tego celu nie jest wymagany.

Warunki przełączenia

Klaster trybu failover przełącza zarządzanie ochroną urządzeń klienckich z węzła aktywnego na 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. Zainstaluj i skonfiguruj serwer NFS:
   - Dostęp do serwera plików musi być włączony dla obu węzłów w ustawieniach serwera NFS.
   - Protokół NFS musi mieć wersję 4.0 lub 4.1.
   - Minimalne wymagania dla jądra Linux:
     - 3.19.0-25, jeśli używasz NFS 4.0
     - 4.4.0-176, jeśli używasz NFS 4.1

3. Na serwerze plików utwórz dwa foldery i udostępnij je przy użyciu systemu plików NFS. 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.

   Uruchom następujące polecenia:

   ```
   sudo yum install nfs-utils
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >>
   /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo cat /etc/exports
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo service nfs start
   ```

   Włącz autostart, uruchamiając następujące polecenie:

   ```
   sudo systemctl enable rpcbind
   ```

4. Uruchom ponownie serwer plików.

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. Aby węzły działały jako klienci NFS, zainstaluj pakiet nfs-utils na każdym węźle.

   Uruchom następujące polecenie:

   ```
   sudo yum install nfs-utils
   ```

3. Utwórz punkty montowania, uruchamiając następujące polecenia:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. Sprawdź, czy współdzielone foldery mogą zostać pomyślnie zamontowane. [krok opcjonalny]

   Uruchom następujące polecenia:

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {server}:{path to
   the KlFocStateShare folder} /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {server}:{path to
   the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc
   ```

Tutaj {server}:{path to the KlFocStateShare folder} oraz {server}:{path to the KlFocDataShare_klfoc folder} są ścieżkami sieciowymi do folderów współdzielonych na serwerze plików.

Po pomyślnym zamontowaniu folderów współdzielonych odmontuj je, uruchamiając następujące polecenia:

```
sudo umount /mnt/KlFocStateShare
sudo umount /mnt/KlFocDataShare_klfoc
```

5. Dopasuj punkty montowania i foldery współdzielone:

```
sudo vi /etc/fstab
{server}:{path to the KlFocStateShare folder} /mnt/KlFocStateShare nfs
vers=4,nolock,local_lock=none,auto,user,rw 0 0
{server}:{path to the KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc nfs
vers=4,nolock,local_lock=none,noauto,user,rw 0 0
```

Tutaj {server}:{path to the KlFocStateShare folder} oraz {server}:{path to the KlFocDataShare_klfoc folder} są ścieżkami sieciowymi do folderów współdzielonych na serwerze plików.

6. Zrestartuj oba węzły.

7. Zamontuj foldery współdzielone, uruchamiając następujące polecenia:

```
mount /mnt/KlFocStateShare
mount /mnt/KlFocDataShare_klfoc
```

8. Upewnij się, że uprawnienia dostępu do folderów udostępnionych należą do ksc:kladmins.

Uruchom następujące polecenie:

```
sudo ls -la /mnt/
```

9. Wykonaj jedną z poniższych czynności:

- W każdym z węzłów utwórz wirtualną kartę sieciową. Na przykład uruchom następujące polecenia:

a. Odkryj nazwy interfejsów, uruchamiając następujące polecenie:

```
ifconfig
```

b. Uruchom następujący skrypt (w dalszej części nazwy interfejsów podano jako przykłady):

```
#!/bin/bash

PHYSICAL_IFACE=ens160
VIRTUAL_IFACE=macvlan1

ip link del $VIRTUAL_IFACE > /dev/null 2>&1

ip link add link $PHYSICAL_IFACE $VIRTUAL_IFACE type macvlan
jeśli [ "$?" -ne "0" ]; następnie
 echo ERROR podczas dodawania nowego wirtualnego adaptera $VIRTUAL_IFACE!
 exit $?
fi

ip link set $VIRTUAL_IFACE down
jeśli [ "$?" -ne "0" ]; następnie
 echo BŁĄD wyłączający wirtualny adapter $VIRTUAL_IFACE!
 exit $?
fi
```

c. Uruchom następujące polecenie:

```
ip addr add { adres IP wirtualnej karty sieciowej } dev { nazwa wirtualnej
karty sieciowej }
```

Adres IP musi być pusty podczas tworzenia wirtualnej karty sieciowej. Wirtualne karty sieciowe w obu węzłach muszą mieć ten sam adres IP.

d. Sprawdź, czy wirtualna karta sieciowa została pomyślnie utworzona.

Uruchom następujące polecenia:

```
ip link set macvlan1 up
ifconfig
```

e. Wyłącz wirtualną kartę sieciową, uruchamiając następujące polecenie:

```
ip link set macvlan1 down
```

- 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.

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

Ta procedura opisuje sposób instalacji Kaspersky Security Center na węzłach klastra 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.

Użyj pliku instalacyjnego — ksc64_[version_number]_amd64.deb lub ksc64-[version_number].x86_64.rpm — który odpowiada dystrybucji Linux zainstalowanej na urządzeniu. Plik instalacyjny można pobrać ze strony internetowej Kaspersky.

Tylko użytkownik z grupy domen KLAdmins może zainstalować Kaspersky Security Center na każdym węźle.

Instalacja na węźle podstawowym (aktywnym)

W celu zainstalowania Kaspersky Security Center na węźle podstawowym:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center, działa jedna z obsługiwanych dystrybucji systemu Linux.

2. W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

3. Uruchom instalację Kaspersky Security Center. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

- `sudo apt install /<path>/ksc64_[version_number]_amd64.deb`
- `sudo yum install /<path>/ksc64-[version_number].x86_64.rpm -y`

4. Uruchom konfigurację Kaspersky Security Center:

   `sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`

5. Przeczytaj Umowę Licencyjną Użytkownika Końcowego (EULA) i Politykę prywatności. Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź następujące wartości:

   a. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki umowy licencyjnej. Wpisz `n`, jeśli nie akceptujesz warunków umowy licencyjnej. Aby korzystać z Kaspersky Security Center, musisz zaakceptować warunki umowy licencyjnej.

   b. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Polityki Prywatności oraz zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności. Wpisz `n`, jeśli nie akceptujesz warunków Polityki Prywatności. Aby korzystać z Kaspersky Security Center, musisz zaakceptować warunki Polityki prywatności.

6. Wybierz **Podstawowy węzeł klastra** jako tryb instalacji Serwera administracyjnego.

7. Po wyświetleniu monitu wprowadź następujące ustawienia:

   a. Wprowadź ścieżkę lokalną do punktu podłączenia dzielenia stanu.

   b. Wprowadź ścieżkę lokalną do punktu podłączenia dzielenia danych.

   c. Wybierz tryb łączności klastra pracy awaryjnej (failover): za pośrednictwem wirtualnej karty sieciowej lub zewnętrznego modułu równoważenia obciążenia.

   d. Jeśli używasz wirtualnej karty sieciowej, wprowadź jej nazwę.

   e. Gdy pojawi się monit o podanie nazwy DNS serwera administracyjnego lub statycznego adresu IP, wprowadź adres IP wirtualnej karty sieciowej lub adres IP zewnętrznego modułu równoważenia obciążenia.

   f. Wprowadź numer portu Serwera administracyjnego. Domyślnie wykorzystywany jest port 14000.

   g. Wprowadź numer portu SSL Serwera administracyjnego. Domyślnie wykorzystywany jest port 13000.

   h. Oceń przybliżoną liczbę urządzeń, którymi zamierzasz zarządzać:

      - Jeśli masz od 1 do 100 urządzeń sieciowych, wpisz 1.
      - Jeśli masz od 101 do 1000 urządzeń sieciowych, wpisz 2.
      - Jeśli masz więcej niż 1000 urządzeń sieciowych, wpisz 3.

   i. Wprowadź nazwę grupy zabezpieczeń dla usług. Domyślnie używana jest grupa „kladmins”.

   j. Wprowadź nazwę konta, aby uruchomić usługę Serwera administracyjnego. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „ksc”.

   k. Wprowadź nazwę konta, aby uruchomić inne usługi. Konto musi należeć do wprowadzonej grupy zabezpieczeń. Domyślnie używane jest konto „ksc”.

l. Wprowadź adres IP urządzenia, na którym zainstalowana jest baza danych.

m. Wprowadź numer portu bazy danych. Ten port jest używany do komunikacji z Serwerem administracyjnym. Domyślnie wykorzystywany jest port 3306.

n. Wprowadź nazwę bazy danych.

o. Wprowadź login konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

p. Wprowadź hasło konta głównego bazy danych, którego używasz do uzyskiwania dostępu do bazy danych.

Poczekaj, aż usługi zostaną dodane i uruchomione automatycznie:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. Utwórz konto, które będzie działać jako administrator Serwera administracyjnego. Wprowadź nazwę użytkownika i hasło. Hasło użytkownika nie może mieć mniej niż 8 ani więcej niż 16 znaków.

Użytkownik zostanie dodany, a Kaspersky Security Center zostanie zainstalowany na węźle podstawowym.

Instalacja na węźle dodatkowym (pasywnym)

W celu zainstalowania Kaspersky Security Center na węźle dodatkowym:

1. Upewnij się, że na urządzeniu, na którym chcesz zainstalować Kaspersky Security Center, działa jedna z obsługiwanych dystrybucji systemu Linux.

2. W wierszu poleceń uruchom polecenia podane w tej instrukcji na koncie z uprawnieniami administratora.

3. Uruchom instalację Kaspersky Security Center. W zależności od dystrybucji Linux uruchom jedno z następujących poleceń:

   - `sudo apt install /<path>/ksc64_[version_number]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[version_number].x86_64.rpm -y`

4. Uruchom konfigurację Kaspersky Security Center:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Przeczytaj Umowę Licencyjną Użytkownika Końcowego (EULA) i Politykę prywatności. Tekst jest wyświetlany w oknie wiersza poleceń. Naciśnij spację, aby wyświetlić następny segment tekstu. Następnie po wyświetleniu monitu wprowadź następujące wartości:

   a. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki umowy licencyjnej. Wpisz `n`, jeśli nie akceptujesz warunków umowy licencyjnej. Aby korzystać z Kaspersky Security Center, musisz zaakceptować warunki umowy licencyjnej.

   b. Wpisz `y`, jeśli rozumiesz i akceptujesz warunki Polityki Prywatności oraz zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności. Wpisz `n`, jeśli nie

akceptujesz warunków Polityki Prywatności. Aby korzystać z Kaspersky Security Center, musisz zaakceptować warunki Polityki prywatności.

6. Wybierz **Dodatkowy węzeł klastra** jako tryb instalacji Serwera administracyjnego.

7. Po wyświetleniu monitu wprowadź ścieżkę lokalną do punktu montowania dzielenia stanu.

Kaspersky Security Center jest zainstalowany na aktywnym węźle.

Weryfikacja usługi

Użyj następujących poleceń, aby sprawdzić, czy usługa jest uruchomiona:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

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. W aktywnym węźle przejdź do /opt/kaspersky/ksc64/sbin.

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, którym chcesz zarządzać, przejdź do /opt/kaspersky/ksc64/sbin.
3. Otwórz wiersz poleceń, a następnie odłącz węzeł od klastra, uruchamiając polecenie `detach_node.sh`.
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 utrzymywanym węźle przejdź do /opt/kaspersky/ksc64/sbin.
8. Otwórz wiersz poleceń, a następnie dołącz węzeł do klastra, uruchamiając polecenie `attach_node.sh`.
9. W węźle aktywnym uruchom klaster trybu failover za pomocą polecenia `klfoc -startcluster --stp klfoc`.

Węzeł jest utrzymywany i dołączany do klastra trybu failover.

Certyfikaty do pracy z Kaspersky Security Center

Ta sekcja zawiera informacje o certyfikatach Kapsersky Scurity Center i opisuje sposób wystawiania i zastępowania certyfikatów dla konsoli internetowej Kaspersky Security Center 14 Web Console oraz odnawiania certyfikatu dla serwera administracyjnego, jeśli serwer współpracuje z konsolą internetową Kaspersky Security Center 14 Web Console.

Informacje o certyfikatach Kaspersky Security Center

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

- Certyfikatu Serwera administracyjnego
- Certyfikat serwera sieciowego
- Certyfikat Kaspersky Security Center 14 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 Kaspersky Security Center 14 Web Console, 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

Certyfikaty Serwera administracyjnego

Certyfikat Serwera administracyjnego jest wymagany do następujących celów:

- Uwierzytelnianie Serwera administracyjnego podczas łączenia się z Kaspersky Security Center 14 Web Console
- Bezpieczna interakcja pomiędzy Serwerem administracyjnym a Agentem sieciowym na zarządzanych urządzeniach
- Uwierzytelnianie, gdy główne Serwery administracyjne są połączone z dodatkowymi Serwerami administracyjnymi

Certyfikat Serwera administracyjnego jest tworzony automatycznie w trakcie instalacji modułu Serwera administracyjnego i jest przechowywany w folderze /var/opt/kaspersky/klnagent_srv/1093/cert/. Certyfikat Serwera administracyjnego określasz podczas tworzenia pliku odpowiedzi w celu zainstalowania Kaspersky Security Center 14 Web Console. Ten certyfikat jest nazywany standardowym („C").

Certyfikat Serwera administracyjnego jest ważny przez 397 dni. Kaspersky Security Center automatycznie generuje wspólny certyfikat rezerwowy („CR") 90 dni przed wygaśnięciem certyfikatu wspólnego. 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.

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

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.

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.

Certyfikat serwera sieciowego

Specjalny typ certyfikatu jest używany przez serwer sieciowy, komponent Serwer administracyjny Kaspersky Security Center. Ten certyfikat jest wymagany do publikowania pakietów instalacyjnych Agenta sieciowego, które są następnie pobierane na zarządzane urządzenia. W tym celu serwer sieciowy może użyć różnych certyfikatów.

Serwer sieci Web używa jednego z następujących certyfikatów, w kolejności priorytetu:

1. Niestandardowy certyfikat serwera sieciowego, który określono ręcznie za pomocą Kaspersky Security Center 14 Web Console

2. Niestandardowy certyfikat Serwera administracyjnego („C”)

Certyfikat Kaspersky Security Center 14 Web Console

Serwer Kaspersky Security Center 14 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.

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 serwera sieciowego	Rozszerzone użycie klucza: uwierzytelnianie serwera. Kontener PKCS #12 / PEM, z którego certyfikat jest określony, zawiera cały łańcuch kluczy publicznych.	Nienadająca się do zastosowania.

	Alternatywna nazwa podmiotu (SAN) certyfikatu jest obecna; czyli wartość pola `subjectAltName` jest ważna. Certyfikat spełnia faktyczne wymagania przeglądarek internetowych nałożone na certyfikaty serwera, a także bieżące podstawowe wymagania CA/Browser Forum.	
Certyfikat Kaspersky Security Center 14 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 internetowych nałożone na certyfikaty serwera, a także bieżące podstawowe wymagania CA/Browser Forum.	Zaszyfrowane certyfikaty nie są obsługiwane przez Kaspersky Security Center 14 Web Console.

Ponowne wystawianie certyfikatu dla Kaspersky Security Center 14 Web Console

Większość przeglądarek nakłada ograniczenie na okres ważności certyfikatu. Okres ważności certyfikatu Kaspersky Security Center 14 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 14 Web Console, który utracił ważność.

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 ponownego opublikowania certyfikatu Kaspersky Security Center 14 Web Console, który utracił ważność:

Zainstaluj ponownie Kaspersky Security Center 14 Web Console, wykonując jedną z następujących czynności:

- Jeśli chcesz użyć tego samego pliku instalacyjnego co Kaspersky Security Center 14 Web Console, usuń Kaspersky Security Center 14 Web Console, a następnie zainstaluj tę samą wersję Kaspersky Security Center 14 Web Console.
- Jeśli chcesz użyć pliku instalacyjnego zaktualizowanej wersji, uruchom polecenie upgrade.

Certyfikat dla Kaspersky Security Center 14 Web Console jest ponownie publikowany dla innego okresu ważności wynoszącego 397 dni.

Zastępowanie certyfikatu dla Kaspersky Security Center 14 Web Console

Domyślnie, gdy instalujesz Kaspersky Security Center 14 Web Console Server (zwany także Kaspersky Security Center 14 Web Console), certyfikat przeglądarki dla aplikacji zostaje wygenerowany automatycznie. Możesz zastąpić automatycznie wygenerowany certyfikat certyfikatem niestandardowym.

W celu zastąpienia certyfikatu dla Kaspersky Security Center 14 Web Console certyfikatem niestandardowym:

1. Utwórz nowy plik odpowiedzi wymagany do instalacji Kaspersky Security Center 14 Web Console.
2. W tym pliku określ ścieżki do niestandardowego pliku certyfikatu i pliku kluczy, używając parametru `certPath` i parametru `keyPath`.
3. Zainstaluj ponownie Kaspersky Security Center 14 Web Console, określając nowy plik odpowiedzi. Wykonaj jedną z poniższych czynności:
   - Jeśli chcesz użyć tego samego pliku instalacyjnego co Kaspersky Security Center 14 Web Console, usuń Kaspersky Security Center 14 Web Console, a następnie zainstaluj tę samą wersję Kaspersky Security Center 14 Web Console.
   - Jeśli chcesz użyć pliku instalacyjnego zaktualizowanej wersji, uruchom polecenie upgrade.

Kaspersky Security Center 14 Web Console działa z określonym certyfikatem.

Konwersja certyfikatu PFX do formatu PEM

Aby użyć certyfikatu PFX w Kaspersky Security Center 14 Web Console, musisz najpierw przekonwertować go do formatu PEM za pomocą dowolnego wygodnego narzędzia wieloplatformowego opartego na OpenSSL.

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 14 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 14 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 internetowa 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 poniżej.

Typ Certyfikatu: Certyfikat standardowy, standardowy certyfikat zapasowy („C", „CR")

Wymagania:

- 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.

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

Etapy

Określanie certyfikatu Serwera administracyjnego odbywa się w etapach:

1. **Zastępowanie certyfikatu Serwera administracyjnego**

   W tym celu użyj polecenia narzędzie klsetsrvcert.

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

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

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.
`-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.

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>]
```

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 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.

Określanie folderu współdzielonego

Po zainstalowaniu Serwera administracyjnego możesz określić lokalizację folderu współdzielonego we właściwościach Serwera administracyjnego. Domyślnie folder współdzielony jest tworzony na urządzeniu z Serwerem administracyjnym. 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.

Informacje o aktualizacji Kaspersky Security Center Linux

Możesz zainstalować Serwer administracyjny w wersji 14 na urządzeniu, na którym jest zainstalowana wcześniejsza wersja Serwera administracyjnego (począwszy od wersji 13). Podczas aktualizowania do wersji 14 wszystkie dane i ustawienia z poprzedniej wersji Serwera administracyjnego zostają zachowane.

Podczas aktualizacji równoczesne korzystanie z DBMS przez Serwer administracyjny i inną aplikację jest surowo zabronione.

Wersję Serwera administracyjnego można zaktualizować, korzystając z jednej z następujących metod:

- Korzystając z pliku instalacyjnego Kaspersky Security Center
- Tworząc kopię zapasową danych Serwera administracyjnego, instalując nową wersję Serwera administracyjnego i przywracając dane Serwera administracyjnego z kopii zapasowej

Jeżeli Twoja sieć zawiera kilka Serwerów administracyjnych, musisz zaktualizować każdy Serwer ręcznie. Kaspersky Security Center Linux nie obsługuje scentralizowanej aktualizacji.

Podczas gdy aktualizujesz Kaspersky Security Center Linux z poprzedniej wersji, wszystkie zainstalowane wtyczki obsługiwanych aplikacji Kaspersky są zachowywane. Wtyczki Serwera administracyjnego i Agenta sieciowego zostają zaktualizowane automatycznie.

Aktualizacja Kaspersky Security Center Linux przy użyciu pliku instalacyjnego

Aby zaktualizować Serwer administracyjny z poprzedniej wersji (począwszy od wersji 13) do wersji 14, możesz zainstalować nową wersję na wcześniejszej przy użyciu pliku instalacyjnego Kaspersky Security Center.

W celu uaktualnienia wcześniejszej wersji Serwera administracyjnego do wersji 14 przy użyciu pliku instalacyjnego:

1. Pobierz plik instalacyjny Kaspersky Security Center z pełnym pakietem dla wersji 14 ze strony internetowej Kaspersky:
   - Dla urządzeń z systemem operacyjnym opartym na RPM — ksc64-<numer wersji>-11247.x86_64.rpm
   - Dla urządzeń z systemem operacyjnym opartym na Debian — ksc64_<numer wersji>-11247_amd64.deb
2. Uaktualnij pakiet instalacyjny za pomocą menedżera pakietów, którego używasz na swoim Serwerze administracyjnym. Na przykład możesz użyć następujących poleceń w terminalu wiersza poleceń na koncie z uprawnieniami roota:
   - W przypadku urządzeń z systemem operacyjnym opartym na RPM:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<numer wersji>-11247.x86_64.rpm
     ```
   - Dla urządzeń z systemem operacyjnym opartym na systemie Debian:
     ```
     $ sudo dpkg -i ksc64_<numer wersji>-11247_amd64.deb
     ```

   Po pomyślnym wykonaniu polecenia tworzony jest skrypt /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl. Komunikat o tym jest wyświetlany w terminalu.

3. Uruchom skrypt /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl w celu skonfigurowania zaktualizowanego Serwera administracyjnego.

4. Przeczytaj Umowę licencyjną i Politykę prywatności, które pojawiają się w terminalu wiersza poleceń. Jeśli zgadzasz się ze wszystkimi warunkami Umowy licencyjnej i Polityki prywatności:

   a. Wpisz „Y”, aby potwierdzić, że w pełni przeczytałeś(-aś), zrozumiałeś(-aś) i akceptujesz warunki umowy EULA.

   b. Wpisz ponownie „Y”, aby potwierdzić, że w pełni przeczytałeś(-aś), zrozumiałeś(-aś) i akceptujesz Politykę prywatności opisującą sposób postępowania z danymi.

   Instalacja aplikacji na Twoim urządzeniu będzie kontynuowana po dwukrotnym wpisaniu „Y”.

5. Wpisz '1', aby wybrać standardowy tryb instalacji Serwera administracyjnego.

   Poniższy obrazek przedstawia dwa ostatnie kroki.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Zaakceptowanie warunków umowy EULA i Polityki prywatności oraz wybranie standardowego trybu instalacji Serwera administracyjnego w terminalu wiersza poleceń

   Następnie instalator konfiguruje i kończy aktualizację Serwera administracyjnego. Podczas aktualizacji nie możesz zmienić ustawień Serwera administracyjnego, które zostały dostosowane przed aktualizacją.

6. Dla urządzeń, na których została zainstalowana 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 Linux.

   Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

Aktualizacja Kaspersky Security Center Linux poprzez kopię zapasową

Aby zaktualizować Serwer administracyjny z poprzedniej wersji (począwszy od wersji 13) do wersji 14, możesz utworzyć kopię zapasową danych Serwera administracyjnego i przywrócić te dane po zainstalowaniu Kaspersky Security Center nowej wersji. Jeżeli podczas instalacji Serwera administracyjnego pojawią się problemy, będzie można przywrócić poprzednią wersję Serwera administracyjnego przy pomocy kopii zapasowej danych Serwera administracyjnego utworzonej przed aktualizacją.

W celu zaktualizowania wcześniejszej wersji Serwera administracyjnego do wersji 14:

1. Przed aktualizacją utwórz kopię zapasową danych Serwera administracyjnego przy użyciu starszej wersji aplikacji.

2. Odinstaluj starszą wersję Kaspersky Security Center.

3. Zainstaluj Kaspersky Security Center w wersji 14 na poprzednim Serwerze administracyjnym.

4. Przywróć dane Serwera administracyjnego z kopii zapasowej utworzonej przed aktualizacją.

5. Dla urządzeń, na których została zainstalowana 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 Linux.

   Po zakończeniu wykonywania zadania zdalnej instalacji, wersja Agenta sieciowego zostanie zaktualizowana.

Logowanie do Kaspersky Security Center 14 Web Console i wylogowywanie

Możesz zalogować się do Kaspersky Security Center 14 Web Console po zainstalowaniu Serwera administracyjnego i serwera konsoli 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.

W celu zalogowania się do Kaspersky Security Center 14 Web Console:

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 dodałeś tylko jeden Serwer administracyjny, zostaną wyświetlone tylko pola Login i Hasło.

3. Wykonaj jedną z poniższych czynności:

   - Aby zalogować się do fizycznego Serwera administracyjnego, wprowadź nazwę użytkownika i hasło lokalnego Administratora.
   - 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.

Po zalogowaniu, zostanie wyświetlony pulpit nawigacyjny zawierający język i motyw, których ostatnio używałeś. Możesz poruszać się po konsoli Kaspersky Security Center 14 Web Console i użyć jej do pracy z Kaspersky Security Center Linux.

W celu wylogowania się z Kaspersky Security Center 14 Web Console:

1. Kliknij nazwę użytkownika znajdującą się w prawym górnym rogu ekranu.

2. Z menu rozwijalnego wybierz **Wyloguj się**.

Konsola Kaspersky Security Center 14 Web Console zostanie zamknięta i zostanie wyświetlona strona logowania.

Kreator wstępnej konfiguracji

Kaspersky Security Center Linux 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 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 antywirusowego, 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 oknie głównym aplikacji kliknij ikonę **Ustawienia** ( ) obok nazwy Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogólne**.
3. Kliknij **Uruchom kreator 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 Kaspersky Security Center Linux.

Zaznacz pole **Użyj serwera proxy**, jeśli podczas łączenia z internetem chcesz korzystać z serwera proxy. Jeśli to pole jest zaznaczone, dostępne staną się pola do wprowadzenia ustawień. Dla połączenia z serwerem proxy określ następujące ustawienia:

- **Adres**
- **Numer portu**

- 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 (to pole jest dostępne, jeśli pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone)

  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 pole **Uwierzytelnianie na serwerze proxy** jest zaznaczone)

  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.

Krok 2. Wybieranie metody aktywacji aplikacji

Wybierz jedną z poniższych opcji aktywacji Kaspersky Security Center Linux:

- Wprowadzając kod aktywacyjny

  Kod aktywacyjny to unikatowa sekwencja 20 znaków alfanumerycznych. Możesz wprowadzić kod aktywacyjny w celu dodania klucza aktywującego Kaspersky Security Center Linux. 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 sekcji głównego menu **OPERACJE → LICENCJONOWANIE → LICENCJE KASPERSKY**.

- 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 sekcji głównego menu **OPERACJE → LICENCJONOWANIE → LICENCJE KASPERSKY**.

- Odraczając aktywację aplikacji

Jeśli wybierzesz opcję odroczenia aktywacji aplikacji, będziesz mógł dodać klucz licencyjny w późniejszym czasie, wybierając **OPERACJE → LICENCJONOWANIE**.

Podczas pracy z Kaspersky Security Center zainstalowanym z płatnego obrazu AMI lub dla Usage-based monthly billed SKU, nie można określić pliku klucza ani wprowadzić kodu.

Krok 3. 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.

Krok 4. 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 DNS serwera SMTP

- **Port serwera SMTP**

  Numer portu komunikacji serwera SMTP. 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, a ustawienia autoryzacji ESMTP są niedostępne.

Możesz przetestować nowe ustawienia powiadomień e-mail, klikając przycisk **Wyślij wiadomość testową**.

Krok 5. Zamykanie Kreatora wstępnej konfiguracji

Aby zamknąć kreator, kliknij przycisk **Zakończ**.

Po zakończeniu działania Kreatora szybkiego startu możesz uruchomić Kreator wdrażania ochrony, aby automatycznie zainstalować programy ochrony lub Agenta sieciowego na urządzeniach w sieci.

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

Możesz ręcznie uruchomić Kreator wdrażania ochrony w dowolnym momencie.

W celu ręcznego uruchomienia Kreatora wdrażania ochrony:

W oknie głównym aplikacji 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 Linux.

  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.

Określ ustawienie dodatkowe:

Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana

Jeśli ta opcja jest włączona, wybrana aplikacja nie zostanie ponownie zainstalowana, jeśli już jest zainstalowana na tym urządzeniu klienckim.

Jeśli ta opcja jest wyłączona, aplikacja zostanie zainstalowana mimo wszystko.

Domyślnie opcja ta jest włączona.

Krok 6. 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 Linux 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 7. 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 8. 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)**

  Jeśli ta opcja jest zaznaczona, możesz określić konto, z poziomu którego zostanie uruchomiony instalator aplikacji. Możesz określić konto użytkownika, jeśli Agent sieciowy nie został zainstalowany na urządzeniach, dla których zadanie jest zdefiniowane.

  Możesz określić kilka kont użytkowników, na przykład, jeśli żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, dla których zadanie jest zdefiniowane. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

  Jeśli nie dodano żadnego konta, zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

Krok 9. 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.

Konfigurowanie Serwera administracyjnego

Ta sekcja opisuje proces konfiguracji i właściwości Serwera administracyjnego Kaspersky Security Center Linux.

Konfigurowanie połączenia Kaspersky Security Center 14 Web Console z Serwerem administracyjnym

W celu określenia portów połączenia Serwera administracyjnego:

1. W górnej części ekranu 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.

Konfigurowanie listy dozwolonych adresów IP do logowania się do Kaspersky Security Center

Domyślnie użytkownicy mogą logować się do Kaspersky Security Center na dowolnym urządzeniu, na którym można otworzyć Kaspersky Security Center 14 Web Console (zwaną dalej Web Console). 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 Kaspersky Security Center za pomocą konsoli internetowej (Web Console), możesz skonfigurować zaporę sieciową na urządzeniu, na którym zainstalowany jest serwer Web Console Server, przy użyciu standardowych środków systemu operacyjnego. Następnie, jeśli ktoś spróbuje zalogować się do Kaspersky Security Center na jednym urządzeniu, a serwer Web Console Server zostanie zainstalowany na innym urządzeniu, zapora sieciowa zapobiegnie ingerencji intruzów.

- 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 /opt/kaspersky/ksc64/sbin).
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 Syslog 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.

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 oknie głównym 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.

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 górnej części ekranu 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**.

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 tworzenia kopii zapasowej danych za pomocą Kaspersky Security Center 14 Web Console.
- 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 (zazwyczaj /opt/kaspersky/ksc64/sbin/klbackup).

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 kopii zapasowej danych Serwera administracyjnego

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.

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.

W celu utworzenia zadania kopii zapasowej danych Serwera administracyjnego:

1. Przejdź do **URZĄDZENIA**→ **ZADANIA**.

2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator dodawania zadań.

3. W pierwszym kroku kreatora, na liście **Aplikacja** wybierz **Kaspersky Security Center 14**, a na liście **Typ zadania** wybierz **Kopia zapasowa danych Serwera administracyjnego**.

4. W odpowiednim kroku kreatora określ następujące informacje:

   - Folder do przechowywania kopii zapasowych
   - Hasło do kopii zapasowej (opcjonalnie)
   - Maksymalna liczba kopii zapasowych do zapisania

5. 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.

6. Kliknij przycisk **Zakończ**.

Zadanie zostanie utworzone i będzie wyświetlane na liście zadań.

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 (zwykle /opt/kaspersky/ksc64/sbin/klbackup).

   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 hasło i folder docelowy kopii zapasowej, a następnie kliknij przycisk **Dalej**, aby rozpocząć tworzenie kopii zapasowej.

W celu przywrócenia danych Serwera administracyjnego w trybie interaktywnym:

1. Uruchom narzędzie klbackup znajdujące się w folderze instalacyjnym Kaspersky Security Center (zwykle /opt/kaspersky/ksc64/sbin/klbackup). Uruchom narzędzie z tego samego konta, którego użyłeś do zainstalowania Serwera administracyjnego.

   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. Musisz upewnić się, 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 ŚCIEŻKA_DOSTĘPU_DO_KOPII_ZAPASOWEJ`—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 PLIKRAPORTU`—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 HASŁO`—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.

- `-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 i serwera bazy danych 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 14 Web Console lub uruchomić narzędzie klbackup .

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 14 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. Zainstaluj Serwer administracyjny na wybranym urządzeniu.

   Zwróć uwagę, że jeśli przenosisz serwer bazy danych na nowe urządzenie, należy określić adres lokalny jako adres IP urządzenia, na którym zainstalowana jest baza danych (element „h" w instrukcji Instalowanie Kaspersky Security Center). Jeśli chcesz zachować serwer bazy danych na poprzednim urządzeniu, wprowadź adres IP poprzedniego urządzenia w pozycji „h" instrukcji Instalowanie Kaspersky Security Center .

5. 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.

6. Otwórz Kaspersky Security Center 14 Web Console i połącz się z Serwerem administracyjnym.

7. Sprawdź, czy wszystkie urządzenia klienckie są połączone z Serwerem administracyjnym.

8. Odinstaluj Serwer administracyjny i serwer bazy danych z poprzedniego urządzenia.

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 oknie głównym 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 14 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 14 Web Console, aby dodać serwer pomocniczy do listy zaufanych Serwerów administracyjnych**. Następnie będzie można połączyć się z wirtualnym Serwerem administracyjnym w Kaspersky Security Center 14 Web Console.

  1. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center 14 Web Console Server, 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 **Zaufane serwery administracyjne** 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 14 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 14 Web Console.

- Użyj konsoli administracyjnej opartej na programie MMC, aby połączyć się bezpośrednio z serwerem wirtualnym.

Hierarchia Serwerów administracyjnych

W MSP może działać kilka Serwerów administracyjnych. Niewygodne może być zarządzanie kilkoma oddzielnymi Serwerami administracyjnymi, dlatego dobrym wyjściem jest utworzenie hierarchii.

W hierarchii Serwer administracyjny Kaspersky Security Center Linux może działać tylko jako dodatkowy serwer zarządzany przez podstawowy Serwer administracyjny Kaspersky Security Center oparty na systemie Windows lub Kaspersky Security Center Cloud Console.

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.

Tworzenie hierarchii Serwerów administracyjnych: dodawanie podrzędnego Serwera administracyjnego

W hierarchii Serwer administracyjny Kaspersky Security Center Linux może działać tylko jako dodatkowy serwer zarządzany przez podstawowy Serwer administracyjny Kaspersky Security Center oparty na systemie Windows lub Kaspersky Security Center Cloud Console.

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 14 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 przejdź na 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 połączenia 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.

- **Użyj serwera proxy**

  Wybierz tę opcję, jeśli używasz serwera proxy do łączenia się z podrzędnym Serwerem administracyjnym.

  W tym przypadku musisz także określić następujące ustawienia serwera proxy:

  - **Adres**
  - **Nazwa użytkownika**
  - **Hasło**

7. Postępuj zgodnie z instrukcjami Kreatora.

   Po zakończeniu pracy kreatora zostanie utworzona hierarchia „główny/podrzędny". 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 14 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 katalogu /var/opt/kaspersky/klnagent_srv/1093/cert/.

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 14 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 14 Web Console, aby dodać serwer pomocniczy do listy zaufanych Serwerów administracyjnych. Następnie będzie można połączyć się z wirtualnym Serwerem administracyjnym w Kaspersky Security Center 14 Web Console.

1. Na urządzeniu, na którym jest zainstalowany Kaspersky Security Center 14 Web Console Server, 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 **Zaufane serwery administracyjne** 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 14 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 14 Web Console.
- Użyj konsoli administracyjnej opartej na programie MMC, aby połączyć się bezpośrednio z serwerem wirtualnym.

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. 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**Bezpieczeństwo uwierzytelniania**.
4. Na zakładce **Bezpieczeństwo uwierzytelniania** 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**.

Weryfikacja dwuetapowa

Ta sekcja opisuje sposób korzystania z weryfikacji dwuetapowej do zmniejszenia ryzyka nieautoryzowanego dostępu do Kaspersky Security Center 14 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**

   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.

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.

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.

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 dwuetapowej weryfikacji konta

Kaspersky Security Center Linux zapewnia weryfikację dwuetapową dla użytkowników Kaspersky Security Center 14 Web Console. Jeśli weryfikacja dwuetapowa jest włączona dla Twojego konta, za każdym razem, gdy logujesz się do Kaspersky Security Center 14 Web Console, wprowadzasz swoją nazwę użytkownika, hasło i 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 14 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 14 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 14 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 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. 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**:
   - Wybierz opcję **Zażądaj nazwę użytkownika, hasło i kod zabezpieczający (weryfikacja dwuetapowa)**, jeśli chcesz włączyć weryfikację dwuetapową dla konta użytkownika:
     - 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.
     - 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 oknie głównym 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. 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 oknie głównym 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 oknie głównym aplikacji kliknij ikonę **ustawienia** ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Bezpieczeństwo uwierzytelniania** w oknie właściwości, w tabeli wykluczeń weryfikacji dwuetapowej kliknij przycisk **Dodaj**.

3. 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. 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 14 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 oknie głównym 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.

Zmienianie liczby dozwolonych prób wprowadzenia hasła

Użytkownik Kaspersky Security Center Linux 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. Na urządzeniu Serwera administracyjnego uruchom wiersz poleceń systemu Linux.

2. W przypadku narzędzia klscflag uruchom następujące polecenie:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   gdzie N to liczba prób wprowadzenia hasła.

3. Aby zastosować zmiany, uruchom ponownie usługę Serwera administracyjnego.

Maksymalna liczba dozwolonych prób wprowadzenia hasła zostanie zmieniona.

Zmiana poświadczeń DBMS

Czasami może zajść potrzeba zmiany poświadczeń DBMS, na przykład w celu wykonania rotacji poświadczeń ze względów bezpieczeństwa.

Aby zmienić poświadczenia DBMS w środowisku Linux za pomocą narzędzia klsrvconfig:

1. Uruchom wiersz poleceń systemu Linux.

2. Określ narzędzie klsrvconfig w otwartym oknie wiersza poleceń:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

3. Podaj nową nazwę konta. Powinieneś określić poświadczenia konta, które istnieje w DBMS.

4. Wpisz nowe hasło.

5. Podaj nowe hasło w celu potwierdzenia.

Poświadczenia DBMS zostały zmienione.

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 górnej części ekranu 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.

Konfigurowanie interfejsu

Możesz skonfigurować interfejs konsoli Kaspersky Security Center 14 Web Console, aby wyświetlał i ukrywał sekcje i elementy interfejsu, w zależności od używanych funkcji.

W celu skonfigurowania interfejsu Kaspersky Security Center 14 Web Console zgodnie z aktualnie używanym zestawem funkcji:

1. W oknie głównym aplikacji kliknij menu konta.

2. Z menu rozwijalnego wybierz **Opcje interfejsu**.

3. W otwartym oknie **Opcje interfejsu** włącz lub wyłącz wymagane opcje.

4. 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 RAPORTY → ALERTY**.

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. Jeśli wszystkie urządzenia w sieci zostaną wykryte, możesz uzyskać informacje o nich i zarządzać nimi poprzez profile. Regularne przeszukiwania sieci są potrzebne do sprawdzania, czy w sieci są jakiekolwiek nowe urządzenia oraz czy wciąż znajdują się w niej wcześniej wykryte urządzenia.

Wykrywanie urządzeń w sieci odbywa się w etapach:

1. **Wstępne wykrywanie urządzeń**

   Po zakończeniu działania Kreatora szybkiego startu wykonaj ręczne wykrywanie urządzeń.

2. **Konfigurowanie przyszłych przeszukiwań**

   Upewnij się, że przeszukiwanie zakresu IP jest włączone i że terminarz przeszukiwania spełnia potrzeby organizacji. Podczas konfigurowania terminarza przeszukiwania skorzystaj z zaleceń dotyczących częstotliwości przeszukiwania sieci.

   Możesz także włączyć przesukiwanie Zeroconf, jeśli Twoja sieć zawiera urządzenia IPv6.

3. **Konfigurowanie reguł dodawania wykrytych urządzeń do grup administracyjnych (opcjonalne)**

   Jeśli nowe urządzenia pojawią się w Twojej sieci, zostaną wykryte podczas regularnych przeszukiwań i zostaną automatycznie uwzględnione w grupie **Urządzenia nieprzypisane**. Jeśli chcesz, możesz skonfigurować reguły automatycznego przenoszenia tych urządzeń do grupy **Zarządzane urządzenia**. Możesz także utworzyć reguły zatrzymania.

   Jeśli pominiesz ten krok konfigurowania reguły, wszystkie nowo wykryte urządzenia zostaną przeniesione do grupy **Urządzenia nieprzypisane** i tam pozostaną. 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 Linux 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**).

Przeszukiwanie zakresu IP

Kaspersky Security Center próbuje przeprowadzić odwrotne rozwiązanie nazwy dla każdego adresu IPv4 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. Jeśli ta strefa nie jest skonfigurowana, przeszukiwanie podsieci IP nie zwróci wyników.

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.

Jeśli włączone jest tylko przeszukiwanie zakresu IP, Kaspersky Security Center wykryje urządzenia tylko z adresami IPv4. Jeśli Twoja sieć zawiera urządzenia IPv6, włącz odpytywanie urządzeń Zeroconf.

Przeglądanie i modyfikowanie ustawień przeszukiwania zakresu IP

W celu przejrzenia i zmodyfikowania właściwości przeszukiwania zakresu IP:

1. 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. 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. 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.

Kaspersky Security Center może przeszukiwać sieci, które mają urządzenia z adresami IPv6. W takim przypadku zakresy adresów IP nie są określone, a Kaspersky Security Center przeszukuje całą sieć za pomocą zero-configuration networking (zwany również *Zeroconf*). Aby rozpocząć korzystanie z Zeroconf, musisz zainstalować narzędzie avahi-browse na urządzeniu z systemem Linux, które odpytuje sieci — Serwer administracyjny lub punkt dystrybucji.

W celu włączenia przeszukiwania Zeroconf:

1. 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 Kaspersky Security Center zaczyna przeszukiwać sieć. W takim przypadku określone zakresy adresów IP są ignorowane.

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, która może zostać użyta 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, możesz skonfigurować regułę, która przypisze znacznik `[CentOS]` do wszystkich urządzeń działających pod kontrolą systemu operacyjnego CentOS. Następnie możesz użyć tego znacznika podczas tworzenia wyboru urządzeń; pomoże to w sortowaniu wszystkich urządzeń z systemem CentOS 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. Na liście wybierz przycisk radiowy obok znacznika 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.

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. Przejrzyj znaczniki przypisane do urządzenia, z którego chcesz usunąć znacznik.

2. Zaznacz pole obok znacznika, który chcesz usunąć.

3. Kliknij przycisk **Wycofaj przypisanie znacznika**.

4. W otwartym oknie kliknij **Tak**.

Znacznik zostanie usunięty z urządzenia.

Znacznik urządzenia nieprzypisanego został usunięty. Jeśli chcesz, możesz usunąć go ręcznie.

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 głónym przejdź do **URZĄDZENIA** → **ZNACZNIKI**, a następnie kliknij odnośnik **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 sieciowe urządzenia, takie jak nazwa DNS urządzenia lub włączenie urządzenia do podsieci IP.
- **Aplikacje**—obecność Agenta sieciowego na urządzeniu oraz typ, wersja i architektura systemu operacyjnego.
- **Maszyny wirtualne**—urządzenie należy do określonego typu maszyny wirtualnej.
- **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.

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 Linux 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.

Wdrażanie aplikacji Kaspersky

Ta sekcja opisuje sposób zdalnej instalacji aplikacji Kaspersky na urządzeniach klienckich w Twojej organizacji przy użyciu Kaspersky Security Center 14 Web Console.

Scenariusz: Wdrażanie aplikacji Kaspersky

Ten scenariusz wyjaśnia sposób wdrażania aplikacji firmy Kaspersky za pośrednictwem Kaspersky Security Center 14 Web Console. Możesz użyć Kreatora wstępnej konfiguracji i Kreatora wdrażania ochrony lub możesz ręcznie wykonać wszystkie niezbędne kroki.

Wdrożenie aplikacji firmy Kaspersky odbywa się w krokach:

1. **Pobieranie sieciowej wtyczki administracyjnej dla aplikacji**

   Pobierz sieciową wtyczkę administracyjną dla Kaspersky Endpoint Security for Linux z witryny internetowej Kaspersky, a następnie dodaj wtyczkę do Kaspersky Security Center 14 Web Console.

2. **Pobieranie i tworzenie pakietu instalacyjnego dla Agenta sieciowego**

   Pobierz pakiet dystrybucyjny Agenta sieciowego z witryny internetowej Kaspersky, a następnie utwórz pakiet instalacyjny Agenta sieciowego.

   Możesz użyć pobranego pakietu dystrybucyjnego, aby zainstalować Agenta sieciowego lokalnie. W tym celu postępuj zgodnie z instrukcjami zawartymi w dokumentacji Kaspersky Endpoint Security for Linux.

3. **Pobieranie i tworzenie pakietu instalacyjnego dla Kaspersky Endpoint Security for Linux**

   Pobierz pakiet dystrybucyjny Kaspersky Endpoint Security for Linux z witryny internetowej Kaspersky, a następnie utwórz pakiet instalacyjny Kaspersky Endpoint Security for Linux.

4. **Tworzenie autonomicznych pakietów instalacyjnych (opcjonalne)**

   Jeśli nie możesz zainstalować aplikacji firmy Kaspersky przy użyciu Kaspersky Security Center Linux na niektórych urządzeniach, na przykład, na zdalnych urządzeniach pracowników, możesz utworzyć autonomiczne pakiety instalacyjne dla aplikacji. Jeśli używasz pakietów autonomicznych do zainstalowania aplikacji Kaspersky, możesz zignorować krok 5 i 6 poniżej.

5. **Tworzenie, konfigurowanie i uruchamianie zadania zdalnej instalacji**

   Ten krok jest częścią Kreator wdrażania ochrony. 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.

6. **Tworzenie i konfigurowanie zadań**

   Należy skonfigurować zadanie *Aktualizacja* programu Kaspersky Endpoint Security for Linux.

Ten krok jest częścią Kreatora wstępnej konfiguracji: zadanie jest tworzone i konfigurowane automatycznie z domyślnymi ustawieniami. Jeśli nie uruchomiłeś 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).

7. **Tworzenie profili**

   Utwórz zasadę dla Kaspersky Endpoint Security for Linux ręcznie lub za pomocą Kreatora wstępnej konfiguracji. Możesz użyć domyślnych ustawień profilu; możesz także zmodyfikować domyślne ustawienia profilu zgodnie ze swoimi potrzebami w dowolnym momencie.

8. **Sprawdzanie wyników**

   Upewnij się, że wdrożenie zakończyło się pomyślnie: masz zasady i zadania dla każdej aplikacji, a te aplikacje są instalowane na zarządzanych urządzeniach.

Wyniki

Zakończenie scenariusza powoduje, że:

- Zostaną utworzone wszystkie wymagane 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.

Dodawanie wtyczek administracyjnych dla aplikacji Kaspersky

Aby wdrożyć aplikację Kaspersky, taką jak Kaspersky Endpoint Security for Linux, musisz dodać i zainstalować sieciową wtyczkę administracyjną dla aplikacji.

W celu dodania i zainstalowania sieciowej wtyczki administracyjnej dla aplikacji Kaspersky:

1. Pobierz sieciową wtyczkę administracyjną dla Kaspersky Endpoint Security for Linux z witryny internetowej Kaspersky.
2. Otwórz Kaspersky Security Center 14 Web Console
3. Z listy rozwijalnej **Ustawienia konsoli** wybierz **Wtyczki sieciowe**.

   Zostanie wyświetlona lista dostępnych wtyczek zarządzających.
4. Kliknij przycisk **Dodaj z pliku**.

   Zostanie wyświetlone okno **Dodaj z pliku**.
5. Kliknij przycisk **Prześlij plik ZIP**.
6. Określ pobrany plik ZIP wtyczki sieciowej.
7. Kliknij przycisk **Prześlij podpis**.
8. Określ pobrany plik TXT podpisu wtyczki sieciowej.

9. Kliknij przycisk **Dodaj**.

   Kaspersky Security Center weryfikuje przesłane pliki, a następnie dodaje i instaluje wtyczkę sieciową.

10. Po zakończeniu instalacji, kliknij **OK**.

    Sieciowa wtyczka administracyjna zostanie zainstalowana z domyślną konfiguracją i wyświetlona na liście sieciowych wtyczek administracyjnych.

Tworzenie pakietów instalacyjnych z pliku

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.

W celu utworzenia niestandardowego pakietu instalacyjnego:

1. Wykonaj jedną z poniższych czynności:

   - Przejdź do **WYKRYWANIE I WDRAŻANIE → WDRAŻANIE I PRZYPISYWANIE → PAKIETY INSTALACYJNE**.
   - 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**.

5. W oknie, które zostanie otwarte, 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).

   Rozpocznie się przesyłanie pliku do Serwera administracyjnego.

6. Jeśli określono plik aplikacji Kaspersky, możesz otrzymać prośbę o przeczytanie i zaakceptowanie Umowy Licencyjnej Użytkownika Końcowego (EULA) dla aplikacji. Aby kontynuować, musisz zaakceptować umowę licencyjną. Wybierz opcję **Zaakceptuj warunki i postanowienia niniejszej Umowy licencyjnej użytkownika końcowego** tylko wtedy, gdy w pełni przeczytano, zrozumiano warunki umowy EULA i je akceptujesz.

Dodatkowo możesz otrzymać prośbę o przeczytanie i zaakceptowanie Polityki Prywatności. Aby kontynuować, musisz zaakceptować Politykę prywatności. Wybierz opcję **Akceptuję Politykę prywatności**tylko wtedy, gdy rozumiesz i zgadzasz się, że Twoje dane będą przetwarzane i przekazywane (w tym do krajów trzecich) zgodnie z Polityką Prywatności.

7. 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.

8. 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 parametry wiersza polecenia.

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, przesłać w wiadomości e-mail lub przenieść na urządzenie klienckie w inny sposób. Na urządzeniu klienckim użytkownik może uruchomić otrzymany plik lokalnie, aby zainstalować aplikację bez udziału Kaspersky Security Center Linux. Możesz tworzyć autonomiczne pakiety instalacyjne dla aplikacji Kaspersky i aplikacji innych firm. Aby utworzyć autonomiczny pakiet instalacyjny dla aplikacji firmy trzeciej, należy utworzyć niestandardowy pakiet instalacyjny.

Upewnij się, że autonomiczny pakiet instalacyjny nie jest dostępny dla innych osób.

W celu utworzenia autonomicznego pakietu instalacyjnego:

1. Wykonaj jedną z poniższych czynności:

   - Przejdź do **WYKRYWANIE I WDRAŻANIE → WDRAŻANIE I PRZYPISYWANIE → PAKIETY INSTALACYJNE**.
   - 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 wybrana opcja **Nie przenoś urządzeń**. Jeśli chcesz przenieść urządzenie klienckie do dowolnej grupy administracyjnej po zainstalowaniu Agenta sieciowego, nie zmieniaj wyboru opcji.

   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 PkgInst folderu współdzielonego Serwera administracyjnego. Możesz przejrzeć listę pakietów autonomicznych, klikając przycisk **Wyświetl listę pakietów autonomicznych** nad listą pakietów instalacyjnych.

Przeglądanie listy autonomicznych pakietów instalacyjnych

Możesz przejrzeć listę autonomicznych pakietów instalacyjnych i właściwości każdego autonomicznego pakietu instalacyjnego.

W celu przejrzenia listy autonomicznych pakietów instalacyjnych dla wszystkich pakietów instalacyjnych:

Nad listą kliknij przycisk **Wyświetl listę pakietów autonomicznych**.

Na liście autonomicznych pakietów instalacyjnych wyświetlane są ich następujące właściwości:

- **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:

- 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**.

Instalowanie aplikacji przy pomocy zadania zdalnej instalacji

Kaspersky Security Center Linux 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 dodawania zadań.

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 dodawania 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 folder zagnieżdżony, 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 dodawania 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 14 Linux 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 14 Linux 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 14 Linux 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.

Zastępowanie aplikacji zabezpieczających firm trzecich

Instalacja aplikacji zabezpieczających Kaspersky poprzez Kaspersky Security Center Linux może wymagać usunięcia oprogramowania firmy trzeciej niekompatybilnego z instalowaną aplikacją. Kaspersky Security Center oferuje kilka sposobów usunięcia aplikacji firm trzecich.

Usuwanie niekompatybilnych aplikacji podczas konfigurowania zdalnej instalacji aplikacji

Możesz włączyć opcję **Automatycznie odinstaluj niekompatybilne aplikacje**, gdy konfigurujesz zdalną instalację aplikacji zabezpieczającej w Kreatorze wdrażania ochrony. Jeśli ta opcja jest włączona, Kaspersky Security Center usunie niekompatybilne aplikacje przed zainstalowaniem aplikacji zabezpieczającej na zarządzanym urządzeniu.

Instrukcje: 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.

Dostępne instrukcje: Tworzenie zadania

Zdalne usuwanie aplikacji lub aktualizacji oprogramowania

Aplikacje lub aktualizacje oprogramowania na zarządzanych urządzeniach z systemem Linux można usuwać zdalnie tylko za pomocą Agenta sieciowego.

W celu zdalnego usunięcia aplikacji lub aktualizacji oprogramowania z wybranych urządzeń:

1. W oknie głównym aplikacji przejdź do **URZĄDZENIA → ZADANIA**.
2. Kliknij **Dodaj**.

   Zostanie uruchomiony Kreator dodawania zadań. Przejdź przez kroki kreatora, korzystając z przycisku **Dalej**.
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.

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 operacyjnych Linux.

Zalecane jest włączenie tej opcji, jeśli zadanie zostało przypisane do urządzeń, na których zainstalowano Agenty sieciowe.

- Przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny

  Opcja jest przestarzała. Zamiast tego użyj opcji **Przy użyciu Agenta sieciowego** lub **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**.

  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 dezinstalacji są stosowane do systemu operacyjnego urządzenia klienckiego. Jeśli ustawienia nie są stosowane, Kaspersky Security Center nie przesyła plików i nie próbuje odinstalować aplikacji. Na przykład, aby odinstalować aplikację Windows z urządzeń grupy administracyjnej, która zawiera urządzenia działające pod kontrolą różnych systemów operacyjnych, możesz przypisać zadanie dezinstalacji 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).

- 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)**

     Jeśli ta opcja jest zaznaczona, możesz określić konto, z poziomu którego zostanie uruchomiony instalator aplikacji. Możesz określić konto użytkownika, jeśli Agent sieciowy nie został zainstalowany na urządzeniach, dla których zadanie jest zdefiniowane.

     Możesz określić kilka kont użytkowników, na przykład, jeśli żadne z nich nie ma wszystkich wymaganych uprawnień na wszystkich urządzeniach, dla których zadanie jest zdefiniowane. W tym przypadku wszystkie dodane konta są używane do uruchomienia zadania, zaczynając od góry.

     Jeśli nie dodano żadnego konta, zadanie zostanie uruchomione z poziomu konta, z którego uruchomiona jest usługa Serwera administracyjnego.

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.

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, możesz utworzyć własny skrypt — użyj dowolnej wygodnej dla siebie metody.

Po przygotowaniu urządzenia SUSE Linux Enterprise Server 15 wdróż i zainstaluj Agenta sieciowego.

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 Linux 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 dodawania klucza licencyjnego 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. Włączyłeś opcję **Klucz licencyjny rozesłany automatycznie** dla wszystkich trzech kluczy licencyjnych. Aplikacja zabezpieczająca Kaspersky — na przykład Kaspersky Endpoint Security for Linux — 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:

- 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.

Instrukcje: 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:

- 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 14 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 dodawania zadań.

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 Linux 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 później ręcznie rozpowszechniać klucz licencyjny.

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.

Usuwanie klucza licencyjnego z repozytorium

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. Przejdź do **OPERACJE → LICENCJONOWANIE → LICENCJE KASPERSKY**.
2. Wybierz plik klucza lub kod aktywacyjny, który chcesz usunąć z repozytorium.
3. Kliknij przycisk **Usuń**.
4. Potwierdź działanie, klikając przycisk **OK**.

   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.

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 RAPORTY → 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 14 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 14 Linux 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 14 Web Console
- Zakończono 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

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.

2. **Konfigurowanie zadań zdalnego zarządzania aplikacjami firmy Kaspersky**

   Sprawdź zadania utworzone przy pomocy Kreatora wstępnej konfiguracji i dostosuj je (jeśli to konieczne).

   Jak to zrobić: Konfigurowanie grupowego zadania aktualizacji Kaspersky Endpoint Security

   Jeśli to konieczne, utwórz dodatkowe zadania do zarządzania aplikacjami 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.

   Jak to zrobić: ustawianie 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.

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.

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.

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 pomyślnie zainstalowano Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center 14 Web Console. Możesz wziąć pod uwagę zarządzanie ochroną skoncentrowaną na użytkowniku jako alternatywę lub dodatkową opcję dla metody skoncentrowanej na urządzeniu. Dowiedz się więcej na temat dwóch metod zarządzania.

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.

   Jeśli konfigurujesz ochronę swojej sieci w Kreatorze wstępnej konfiguracji, Kaspersky Security Center tworzy domyślny profil dla Kaspersky Endpoint Security for Linux. Jeśli zakończyłeś proces konfiguracji przy użyciu tego kreatora, nie musisz tworzyć nowego profilu dla tej aplikacji.

   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 zasad umożliwi efektywne zarządzanie urządzeniami w grupach administracyjnych.

   Dostępne instrukcje: 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 z określoną konfiguracją sprzętową lub oznaczoną określonymi znacznikami. Użyj znaczników do filtrowania urządzeń, które spełniają określone kryteria. Na przykład możesz utworzyć znacznik nazwany *CentOS*, oznaczyć tym znacznikiem wszystkie urządzenia działające pod kontrolą systemu operacyjnego CentOS, a następnie określić ten znacznik jako warunek aktywacji profilu zasad. W wyniku tego działania aplikacje Kaspersky zainstalowane na wszystkich urządzeniach działających pod kontrolą systemu CentOS będą zarządzane przez własny profil zasad.

   Dostępne instrukcje:

   - Tworzenie profilu zasad
   - Tworzenie reguły aktywacji profilu zasad

3. **Przesyłanie profili i profili zasad na zarządzane urządzenia**

   Domyślnie Kaspersky Security Center automatycznie synchronizuje Serwer administracyjny 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 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.

Wymagania wstępne

Przed rozpoczęciem konfiguracji upewnij się, że pomyślnie zainstalowano Serwer administracyjny Kaspersky Security Center i Kaspersky Security Center 14 Web Console, a także zakończono główny scenariusz wdrażania. 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.

   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 Kaspersky Security Center automatycznie synchronizuje Serwer administracyjny 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.

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**.

Ustawienia zasady Agenta sieciowego

W celu skonfigurowania zasady Agenta sieciowego:

1. W menu głównym przejdź do **URZĄDZENIA** → **ZASADY I PROFILE**.
2. Kliknij nazwę zasady Agenta sieciowego.

   Zostanie otwarte okno właściwości zasady Agenta sieciowego.

Ogólne

Na tej zakładce 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 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 zagnieżdżonych grup 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 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 typowe 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:

- **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 Linux). 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.

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.

- **Szczegóły rejestru sprzętu**

  Agent sieciowy zainstalowany na urządzeniu wysyła informacje o sprzęcie urządzenia do Serwera administracyjnego. Możesz przejrzeć szczegóły sprzętu we właściwościach urządzenia.

Sieć

Sekcja **Sieć** zawiera trzy podsekcje:

- **Łączność**
- **Profile połączenia**
- **Terminarz połączeń**

W podsekcji **Łączność** 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 pulsem) 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.

- **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.

W podsekcji **Profile połączenia** sekcji **Sieć** 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:

- **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

  Profile połączenia są obsługiwane tylko dla urządzeń działających pod kontrolą systemu Windows. Nie zalecamy używać tej opcji.

  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

W grupie ustawień **Profile połączenia** do listy **Profile połączeń Serwera administracyjnego** nie mogą być dodawane żadne nowe elementy, więc przycisk **Dodaj**jest nieaktywny. Predefiniowane profile połączeń także nie mogą być modyfikowane.

- Włącz tryb użytkownika mobilnego, gdy Serwer administracyjny nie jest dostępny

  Jeśli ta opcja jest włączona, w przypadku połączenia przez ten profil, aplikacje zainstalowane na urządzeniu klienckim będą używać profili zasad dla urządzeń w trybie użytkownika mobilnego, a także zasad użytkownika mobilnego. Jeżeli dla aplikacji nie określono zasady użytkownika mobilnego, zostanie użyta zasada aktywna.

  Jeżeli ta opcja jest wyłączona, aplikacje będą używać zasad aktywnych.

  Domyślnie opcja ta jest wyłączona.

W podsekcji **Terminarz połączeń** możesz określić przedziały czasu, w trakcie których Agent sieciowy wysyła dane do Serwera administracyjnego:

- Połącz, gdy jest to konieczne

  Jeśli ta opcja jest zaznaczona, połączenie jest nawiązywane, gdy Agent sieciowy musi wysłać dane na Serwer administracyjny.

  Domyślnie opcja ta jest zaznaczona.

- Połącz w określonych przedziałach czasu

  Jeśli ta opcja jest zaznaczona, Agent sieciowy łączy się z Serwerem administracyjnym w określonym czasie. Możesz dodać kilka przedziałów czasu.

Przeszukiwanie sieci według punktów dystrybucji

W sekcji **Przeszukiwanie sieci według punktów dystrybucji** możesz skonfigurować automatyczne przeszukiwanie sieci. W celu włączenia przeszukiwania sieci i skonfigurowania jego częstotliwości możesz użyć następujących opcji:

- **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.

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**

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).

Zmiana priorytetu reguł przenoszenia urządzeń

Wszystkie reguły przenoszenia urządzeń posiadają priorytety.

W celu zwiększenia lub zmniejszenia priorytetu reguły przenoszenia

przesuń regułę odpowiednio w górę lub w dół listy za pomocą myszy.

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 konsoli Kaspersky Security Center 14 Web Console tylko wtedy, gdy wtyczka zarządzająca dla tej aplikacji jest zainstalowana na serwerze Kaspersky Security Center 14 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 Kaspersky Security Center 14 Web Console 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) 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 dodawania zadań. 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 Linux.

W celu przejrzenia listy zadań,

Przejdź do **URZĄDZENIA**→ **ZADANIA**.

Zostanie wyświetlona lista zadań. Zadania są grupowane według nazw aplikacji, których dotyczą. Na przykład zadanie *Zdalna instalacja aplikacji* dotyczy Serwera administracyjnego, a zadanie *Aktualizacja* odnosi się do Kaspersky Endpoint Security for Linux.

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 wyświetla ustawienia, które możesz przejrzeć i określić dla zadań.

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).

  - **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:
  - 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 w celu zapewnienia wstecznej kompatybilności Kaspersky Security Center Linux.

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 *Aktualizacja*.

- **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.

- **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 urządzenie przed uruchomieniem zadania przy użyciu funkcji Wake-on-LAN (min)**

    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 urządzenie 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, jeśli 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 Syslog 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 Syslog systemu operacyjnego Serwera administracyjnego (OS).

      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.**

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. Na zakładce **URZĄDZENIA** wybierz **ZADANIA**.
2. Kliknij **Zarządzaj poświadczeniami kont do uruchamiania zadań**.

Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Określanie danych uwierzytelniających

Określ nowe poświadczenia, które są aktualnie ważne w Twoim systemie. 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 użytkownik jest aktualnie zalogowany w konsoli Kaspersky Security Center 14 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**.

Przeglądanie wyników wykonywania zadań przechowywanych na Serwerze administracyjnym

Kaspersky Security Center Linux 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 **Ogólne**.
2. Kliknij odnośnik **Wyniki**, aby otworzyć okno **Wyniki zadania**.

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.

Ogólne

Sekcja **Ogólne** wyświetla ogólne informacje o urządzeniu klienckim. Informacje są dostarczane w oparciu o dane otrzymane podczas ostatniej synchronizacji urządzenia klienckiego z Serwerem administracyjnym:

- Nazwa

  W tym polu możesz wyświetlić i zmodyfikować nazwę urządzenia klienckiego w grupie administracyjnej.

- Opis

  W tym polu możesz wprowadzić dodatkowy opis urządzenia klienckiego.

- Grupa

  Grupa administracyjna zawierająca urządzenie klienckie.

- Ostatnia aktualizacja

  Data ostatniej aktualizacji 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.

Sieć

Sekcja **Sieć** wyświetla następujące informacje o właściwościach sieciowych urządzenia klienckiego:

- Adres IP

Adres IP urządzenia.

- Domena Windows

  Grupa robocza zawierająca urządzenie.

- Nazwa DNS

  Nazwa domeny DNS urządzenia klienckiego.

- Nazwa NetBIOS

  Nazwa urządzenia klienckiego.

System

Sekcja **System** zawiera informacje o systemie operacyjnym zainstalowanym na urządzeniu klienckim.

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

  W tym polu jest wyświetlany bieżący stan ochrony w czasie rzeczywistym urządzenia klienckiego.

  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 antywirusowego 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 urządzenia zdefiniowany przez aplikację

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 Linux.

Aplikacje

Sekcja **Aplikacje** wyświetla wszystkie aplikacje firmy Kaspersky zainstalowane 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

Sekcja **Aktywne zasady i profile zasad** zawiera listę zasad i profili zasad, które są aktualnie aktywne na zarządzanym urządzeniu.

Zadania

W sekcji **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

Sekcja **Zdarzenia** wyświetla zdarzenia zarejestrowane na Serwerze administracyjnym dla wybranego urządzenia klienckiego.

Znaczniki

W sekcji **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.

Pliki wykonywalne

Sekcja **Pliki wykonywalne** 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

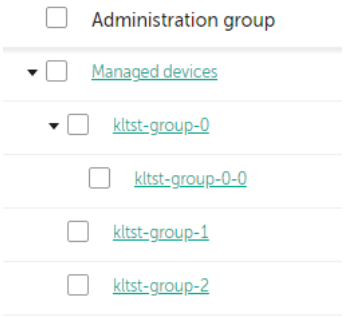
  Kliknij przycisk **Właściwości**, aby przejrzeć i skonfigurować punkt dystrybucji, z którym urządzenie komunikuje się.

Rejestrze sprzętu

W sekcji **Rejestr sprzętu** możesz wyświetlić informacje o sprzęcie zainstalowanym na urządzeniu klienckim.

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 oraz 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. 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.

W celu utworzenia struktury grup administracyjnych:

1. Przejdź do **URZĄDZENIA → HIERARCHIA GRUP**.
2. Kliknij przycisk **Importuj**.

Zostanie uruchomiony Kreator struktury nowej grupy administracyjnej. Postępuj zgodnie z instrukcjami Kreatora.

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. Również reguły przenoszenia urządzeń mogą być tworzone także bezpośrednio przez administratora Kaspersky Security Center Linux w sekcji **URZĄDZENIA → REGUŁY PRZENOSZENIA**.

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 było 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 Linux (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.

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 zakładkę **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. 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. W menu głównym przejdź na zakładkę **URZĄDZENIA → REGUŁY PRZENOSZENIA**.

   Możesz także wybrać opcję **WYKRYWANIE I WDRAŻANIE → WDRAŻANIE I PRZYPISYWANIE** , a następnie z menu wybierz opcję **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.

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 DNS urządzenia**

  Nazwa domeny DNS urządzenia klienckiego, które chcesz przenieść. Wypełnij to pole, jeśli Twoja sieć zawiera serwer DNS.

- **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** lub **Serwer administracyjny Kaspersky Security Center 14**.

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.

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. 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.
     - Podaj nazwę DNS urządzenia.

       Pole nazwy urządzenia nie może zawierać spacji, znaków backspace, a także 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, znaków backspace, a także 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, przejdź do **URZĄDZENIA** → **Grupy** → **<nazwa grupy>** → **ZARZĄDZANE URZĄDZENIA**.
   - Aby otworzyć grupę **URZĄDZENIA NIEPRZYPISANE**, 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.

Zmienianie Serwera administracyjnego dla urządzeń klienckich

Możesz zmienić Serwer administracyjny na inny dla określonych urządzeń klienckich. W tym celu użyj 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.

   Zostanie uruchomiony Kreator dodawania zadań. Postępuj zgodnie z instrukcjami Kreatora. W oknie **Nowe zadanie** Kreatora dodawania zadania wybierz aplikację **Kaspersky Security Center 14** oraz typ zadania **Zmiana Serwera administracyjnego**. Następnie określ urządzenia, dla których chcesz zmienić Serwer administracyjny:

   - **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.

3. Uruchom utworzone zadanie.

Po zakończeniu wykonywania zadania, urządzenia klienckie, dla których zostało ono utworzone, zostaną przekazane Serwerowi administracyjnemu określonemu w ustawieniach zadania.

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 Linux 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 Linux bierze pod uwagę flagę widoczności urządzenia w sieci (patrz tabela poniżej). Jeśli Kaspersky Security Center Linux nie znajdzie urządzenia w sieci w ciągu dwóch godzin, flaga widoczności urządzenia zostanie ustawiona na *Nie jest widoczne.*

Stany są następujące:

- *Krytyczny* lub *Krytyczny / Widoczny*
- *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 skanowania antywirusowego 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 antywirusowe nie było wykonywane od dłuższego czasu	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale zadanie Skanowanie antywirusowe 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.
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.
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 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 Linux 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 Linux z poprzedniej wersji, wartości warunku **Bazy danych są nieaktualne** dla przypisania stanu do *Krytyczne* lub *Ostrzeżenie* nie zmienią się.

Jeśli Kaspersky Security Center Linux 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 otwartym oknie właściwości, w panelu **Sekcje** wybierz **Stan urządzenia**.
3. W sekcji **Ustaw stan Krytyczny, jeśli** zaznacz pole obok warunku na liście.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

4. 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 otwartym oknie właściwości, w panelu **Sekcje** wybierz **Stan urządzenia**.
3. W prawej części, w sekcji **Ustaw stan Ostrzeżenie, jeśli** zaznacz pole obok warunku na liście.

   Możesz zmienić tylko ustawienia, które nie są zablokowane w zasadzie nadrzędnej.

4. 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*.

Profile i profile zasad

W Kaspersky Security Center 14 Web Console możesz tworzyć zasady dla aplikacji firmy 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:

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.
- 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
Undefined	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*.
Enforce	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:

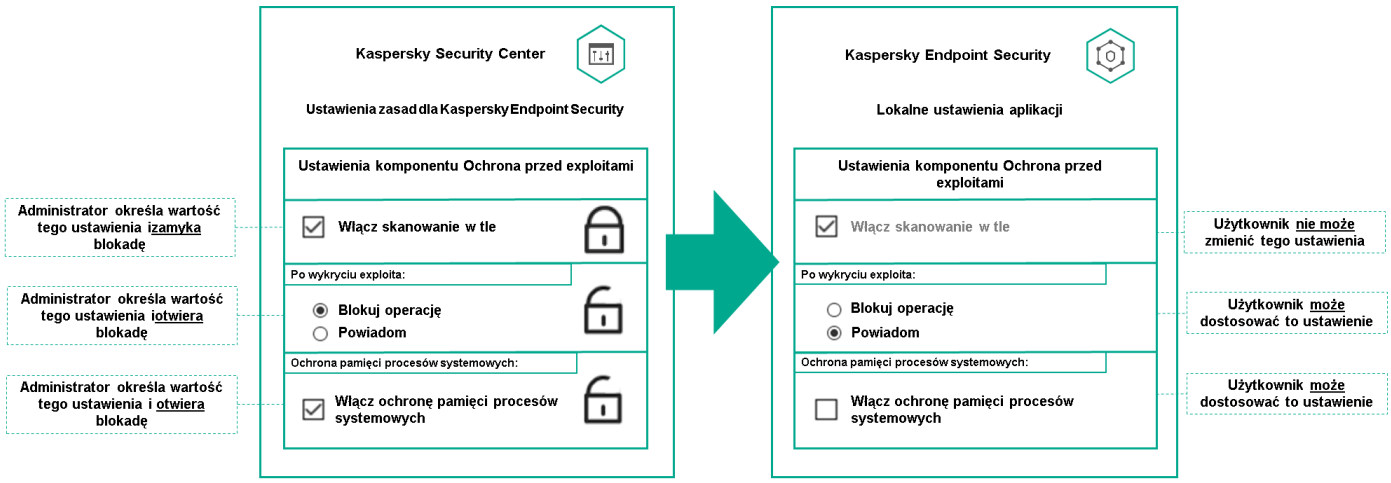
- Blokowanie ustawień dla zasady podgrupy administracyjnej
- Blokowanie ustawień aplikacji Kaspersky na zarządzanym urządzeniu

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 lokalna 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

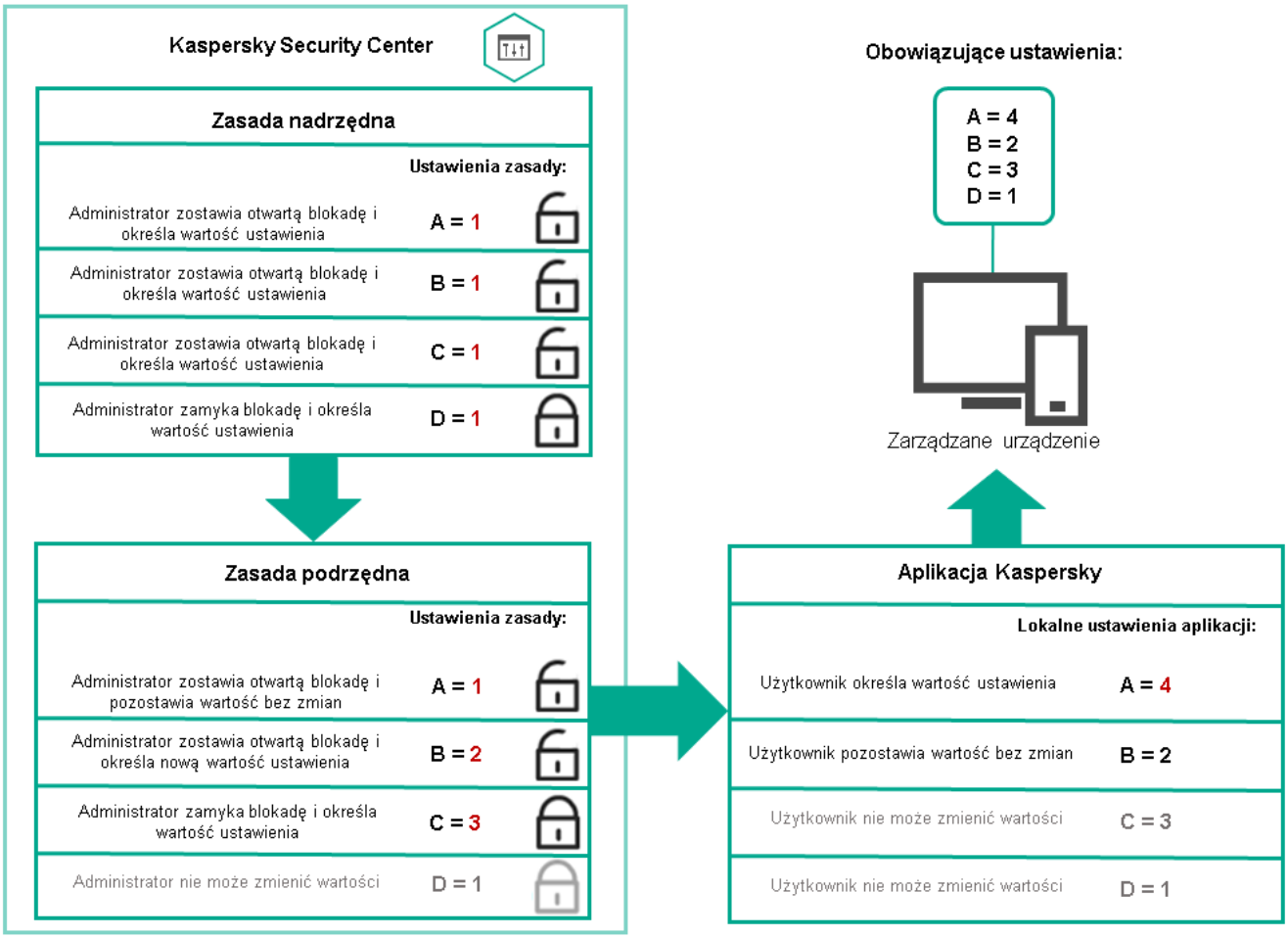
Jeśli różne urządzenia wymagają różnych ustawień, możesz zorganizować je w grupy administracyjne.

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).

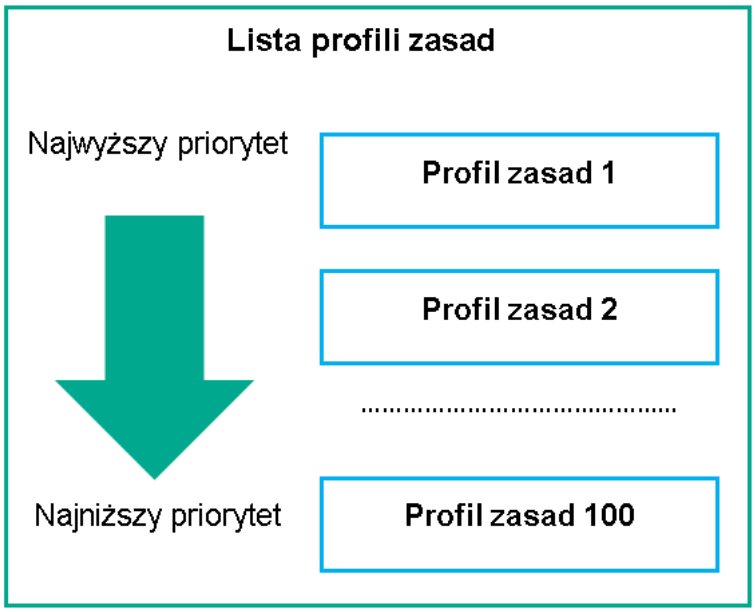


Hierarchia profili

Profile zasad w hierarchii zasad

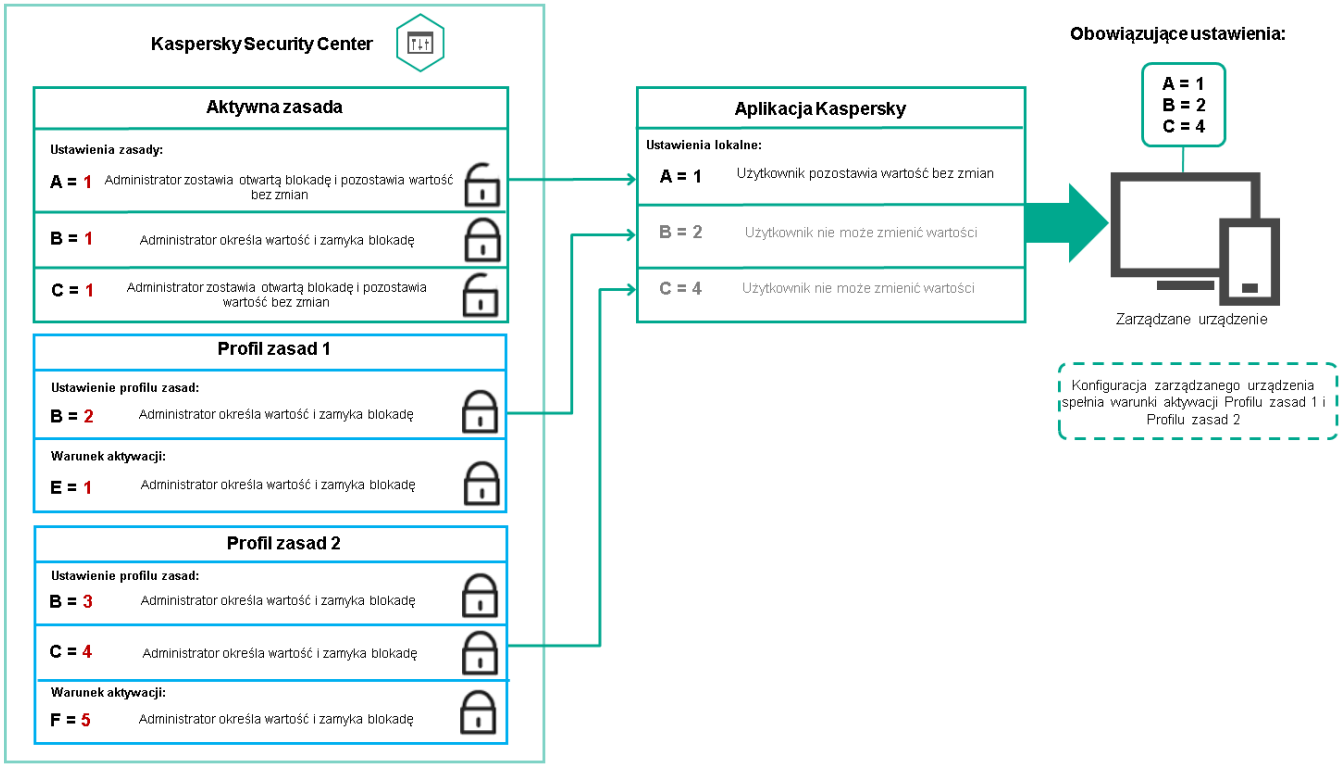
Profile zasad mają następujące warunki przypisywania priorytetów:

- 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).

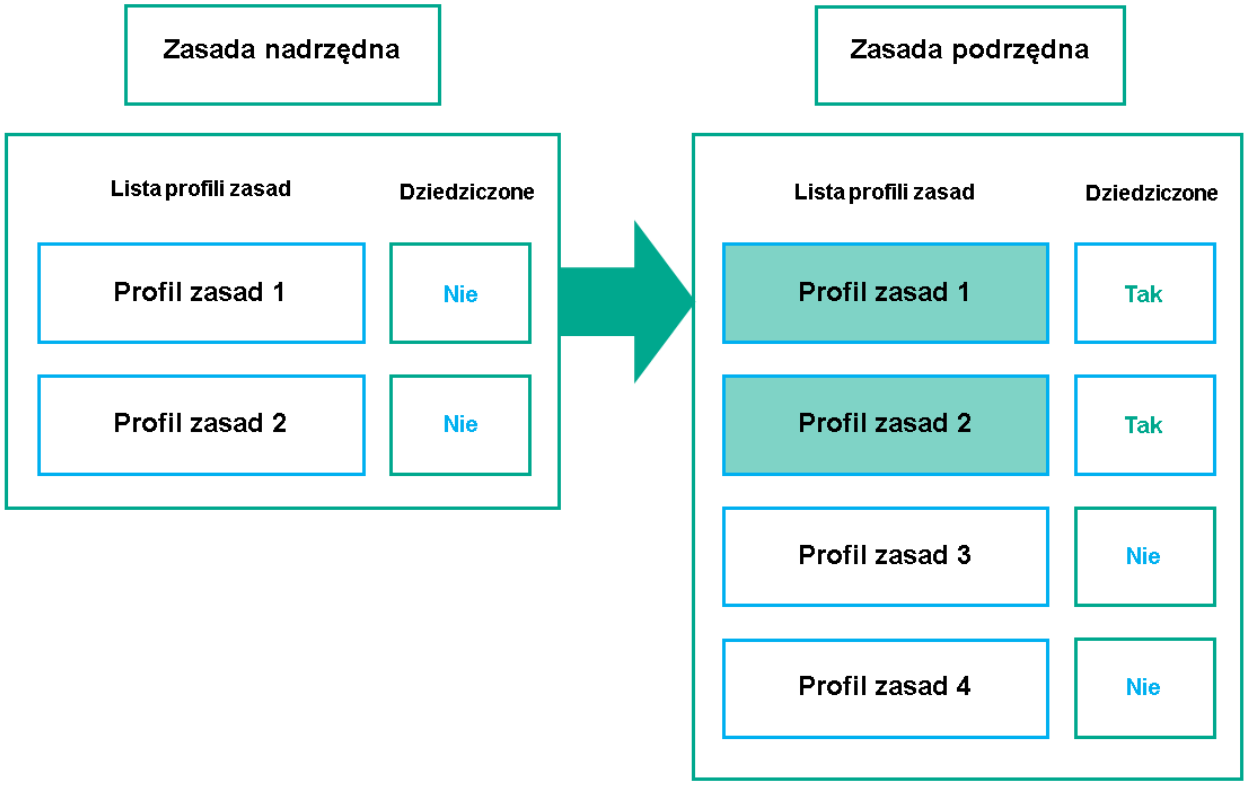


Konfiguracja zarządzanego urządzenia spełnia warunki aktywacji kilku profili zasad

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).

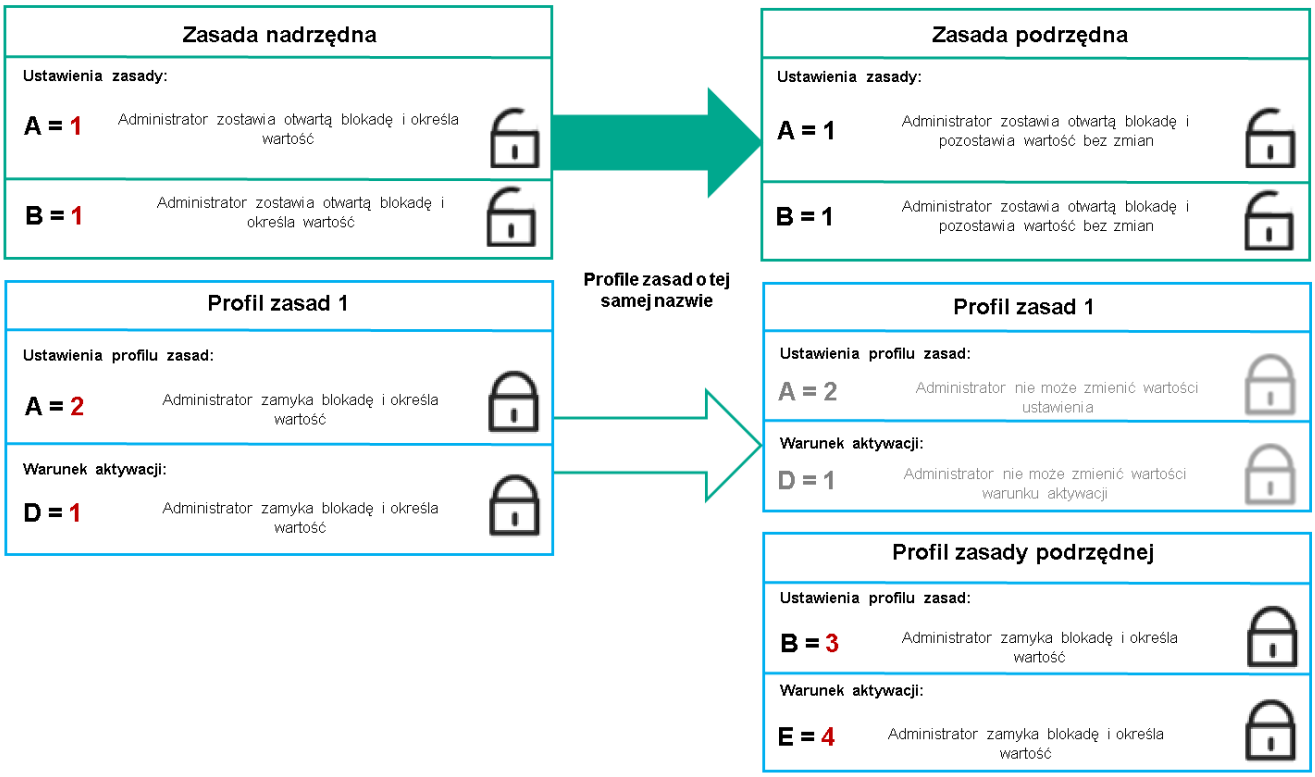


Dziedziczenie profili zasad

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. Przejdź do **URZĄDZENIA → ZASADY I PROFILE**.
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
   - Kaspersky Endpoint Security for Linux — pomoc

   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.

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 zagnieżdżonych grup 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).

Modyfikowanie zasady

W celu zmodyfikowania zasady:

1. Przejdź do **URZĄDZENIA** → **ZASADY I PROFILE**.
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
   - Kaspersky Endpoint Security for Linux — pomoc

   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**.

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 → ZASADY I PROFILE**.
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 → ZASADY I PROFILE**.
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).

Wymuszona synchronizacja

Chociaż Kaspersky Security Center Linux automatycznie synchronizuje stan, ustawienia, zadania i zasady dla zarządzanych urządzeń, to w niektórych przypadkach administrator musi dokładnie wiedzieć, czy w danym momencie dla określonego urządzenia została już przeprowadzona synchronizacja.

Synchronizowanie pojedynczego urządzenia

W celu wymuszenia synchronizacji między Serwerem administracyjnym a zarządzanym urządzeniem:

1. 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:
   - 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. 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.

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. Przejdź do **URZĄDZENIA → ZASADY I PROFILE**.
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. Przejdź do sekcji **Opcje interfejsu** na pasku zadań.
2. W sekcji **Ogranicz urządzenia wyświetlane w wynikach dystrybucji zasady** wprowadź liczbę urządzeń (do 100 000).
   Domyślnie ustawiona jest liczba 5000.
3. Kliknij **Zapisz**.
   Ustawienia zostaną zapisane i zastosowane.

Usuwanie zasady

Możesz usunąć 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 → ZASADY I PROFILE**.
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 przeglądaniu profili zasad, zmienianiu priorytetu profilu zasad, tworzeniu profilu zasad, kopiowaniu profilu zasad, tworzeniu reguły aktywacji profilu zasad i usuwaniu profilu zasad.

Przeglądanie profili zasad

W celu przejrzenia profili zasad:

1. W menu głównym przejdź do **URZĄDZENIA → ZASADY I PROFILE**.
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.

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 Linux. 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 Linux. 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:

  - 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.

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.

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.

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 Linux oferuje możliwości dla dostępu opartego na roli do funkcji Kaspersky Security Center Linux i zarządzanych aplikacji firmy Kaspersky.

Możesz skonfigurować uprawnienia dostępu do funkcji aplikacji dla użytkowników Kaspersky Security Center Linux 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 Linux 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**, **modyfikowania** 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**	**Modyfikuj**	• Dodaj urządzenie do grupy administracyjnej: **Modyfikuj** • Usuń urządzenie z grupy administracyjnej: **Modyfikuj** • Dodaj grupę administracyjną do innej grupy administracyjnej: **Modyfikuj** • Usuń grupę administracyjną z innej grupy administracyjnej: **Modyfikuj**	Brak	Brak
Funkcje ogólne: U**zyskuj 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** • **Modyfikuj** • **Wykonaj** • **Wykonaj operacje na wyborach urządzeń**	• Reguły przenoszenia urządzeń (tworzenie, modyfikowanie lub usuwanie) dla Serwera wirtualnego: **Modyfikuj**, **Wykonuj operacje na wybranych urządzeniach** • Uzyskaj niestandardowy certyfikat protokołu Mobile (LWNGT): **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”

		• Ustaw certyfikat niestandardowy protokołu Mobile (LWNGT): **Zapisz** • Uzyskaj listę sieci zdefiniowaną przez NLA: **Odczytaj** • Dodaj, zmodyfikuj lub usuń listę sieci zdefiniowaną przez NLA: **Modyfikuj** • Wyświetl listę kontroli dostępu grup: **Odczytaj** • Wyświetl dziennik zdarzeń aplikacji Kaspersky: **Odczytaj**		• „Raport o ata sieciowych” • „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 zabronionych aplikacjach” • „Raport Kontr sieci” • „Raport o efektywnych uprawnieniacl użytkowników • „Raport dotyc uprawnień”
Funkcje ogólne: **Obiekty usunięte**	• **Odczyt** • **Modyfikuj**	• Wyświetl usunięte obiekty w Koszu: **Odczytaj**	Brak	Brak

		• Usuń obiekty z Kosza: **Modyfikuj**		
Funkcje ogólne: **Przetwarzanie zdarzeń**	• **Usuń zdarzenia** • **Edytuj ustawienia powiadomień o zdarzeniach** • **Edytuj ustawienia rejestrowania zdarzeń** • **Modyfikuj**	• 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** • **Modyfikuj** • **Wykonaj** • **Modyfikuj listy ACL obiektów** • **Wykonaj operacje na wyborach urządzeń**	• Określ porty Serwera administracyjnego dla połączenia agenta sieciowego: **Modyfikuj** • Określ porty Serwera proxy aktywacji uruchomionego na serwerze administracyjnym Serwer administracyjny: **Modyfikuj** • Określ porty serwera proxy aktywacji dla urządzeń przenośnych uruchomionych na Serwerze administracyjnym: **Modyfikuj** • Określ porty serwera sieciowego do dystrybucji samodzielnych pakietów: **Modyfikuj** • Określ porty serwera	• „Tworzenie kopii zapasowych danych Serwera administracyjnego” • „Konserwacja baz danych”	Brak

		sieciowego do dystrybucji profili MDM: **Modyfikuj** • Określ porty SSL Serwera administracyjnego do połączenia przez Web Console: **Modyfikuj** • Określ porty serwera administracyjnego Serwer administracyjny dla połączenia mobilnego: **Modyfikuj** • Zmienianie maksymalnej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego: **Modyfikuj** • Określ maksymalną liczbę zdarzeń, które mogą być wysłane przez Serwer administracyjny: **Modyfikuj** • Określ przedział czasu, w którym zdarzenia mogą być wysyłane przez Serwer administracyjny: **Modyfikuj**		
Funkcje ogólne: **Wdrażanie oprogramowania Kaspersky**	• **Zarządzaj poprawkami Kaspersky** • **Odczyt** • **Modyfikuj** • **Wykonaj**	Zaakceptuj lub odrzuć instalację poprawki: **Zarządzaj poprawkami Kaspersky**	Brak	• „Raport dotyc użycia klucza licencyjnego p wirtualny serw administracyj • „Raport o wersjach oprogramowa Kaspersky”

	• **Wykonaj operacje na wyborach urządzeń**			• „Raport o niekompatybi aplikacjach” • „Raport o wersjach aktualizacji modułu oprogramowa Kaspersky” • „Raport wdra ochrony”
Cechy ogólne: **Zarządzanie kluczami**	• **Eksportuj plik klucza** • **Modyfikuj**	• Eksportuj plik klucza: **Eksportuj plik klucza** • Zmodyfikuj ustawienia klucza licencyjnego Serwera administracyjnego: **Modyfikuj**	Brak	Brak
Funkcje ogólne: **Wymuszone zarządzanie raportami**	• **Odczyt** • **Modyfikuj**	• 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:	Brak	Brak

		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** • **Modyfikuj** • **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**	Brak	Brak

		serwerami administracyjnymi		

Informacje o rolach użytkowników

Role użytkowników przypisane do użytkowników Kaspersky Security Center Linux 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 predefiniowane role użytkownika dostępne w Kaspersky Security Center Linux mogą być powiązane z określonymi stanowiskami pracy, na przykład **Audytor**, **Pracownik ochrony**, **Nadzorca**. 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 **Modyfikacja** 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.

Funkcje obszarów funkcjonalnych **Zarządzanie urządzeniami mobilnymi: Zarządzanie ogólne** i **Zarządzanie systemem** nie są dostępne w Kaspersky Security Center Linux. Użytkownik z rolami Administrator/ **Operator zarządzania lukami i poprawkami oraz Administrator** / **Operator zarządzania urządzeniami mobilnymi** ma dostęp tylko do uprawnień z funkcji **Ogólne**: **Podstawowy** obszar funkcjonalny.

Prawa dostępu do predefiniowanych ról użytkowników

Rola	Opis
Administrator serwera administracyjnego	Zezwala na następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Podstawowa funkcjonalność** • **Przetwarzanie zdarzeń** • **Hierarchia Serwerów administracyjnych** • **Wirtualne Serwery administracyjne**
Operator serwera administracyjnego	Przyznaje uprawnienia do **odczytu** i **wykonywania** we wszystkich następujących obszarach funkcjonalnych, w **Funkcjach ogólnych:**

	• **Podstawowa funkcjonalność** • **Wirtualne Serwery administracyjne**
Audytor	Zezwala na następujące 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 następujące operacje w obszarach funkcjonalnych, w **Cechach ogólnych**: • **Podstawowa funkcjonalność** • **Zdalna instalacja oprogramowania Kaspersky** • **Zarządzanie kluczami licencyjnymi** 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, w **Funkcjach ogólnych:** • **Podstawowa funkcjonalność** • **Zdalna instalacja oprogramowania Kaspersky** (zapewnia również **Zarządzanie poprawkami Kaspersky Lab** bezpośrednio w tym obszarze) • **Wirtualne Serwery administracyjne**
Administrator Kaspersky Endpoint Security	Zezwala na wszystkie operacje w następujących obszarach funkcjonalnych: • **Cechy ogólne: Podstawowa funkcjonalność** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
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**
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 Lab** • **Wirtualne Serwery administracyjne** • Obszar Kaspersky Endpoint Security zawierający wszystkie funkcje
Administrator zarządzania urządzeniami mobilnymi	Pozwala na wszystkie operacje w obszarze **Funkcje ogólne: Podstawowa funkcjonalność** w obszarze funkcjonalnym.
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**, **modyfikacji**, **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.

Dodawanie konta użytkownika wewnętrznego

W celu dodania nowego konta użytkownika wewnętrznego do Kaspersky Security Center Linux:

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 Linux.

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 Linux:

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 Linux.
     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. W menu głównym przejdź do **UŻYTKOWNICY I ROLE** → **UŻYTKOWNICY**.
2. Kliknij nazwę konta użytkownika, które chcesz przypisać jako właściciel urządzenia.
3. W otwartym oknie ustawień użytkownika kliknij zakładkę **Urządzenia**.
4. Kliknij **Dodaj**.
5. Z listy urządzeń wybierz urządzenie, które chcesz przypisać do użytkownika.
6. 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. Kliknij przycisk **Zamknij** (×), aby zamknąć 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 **Zasady i profile**.
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 rewizjami obiektów

Ta sekcja zawiera informacje dotyczące zarządzania rewizjami obiektów. Kaspersky Security Center Linux 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

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.

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**.

Użycie narzędzia klscflag do otwarcia portu 13291

Port 13291 na serwerze administracyjnym jest używany do odbierania połączeń z konsoli administracyjnych. Na komputerach z systemem innym niż Windows ten port nie jest domyślnie otwarty. Jeśli chcesz używać konsoli administracyjnej opartej na MMC ani narzędzia klakaut, możesz otworzyć ten port za pomocą narzędzia klscflag. To narzędzie zmienia wartość parametru KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Aby otworzyć port 13291:

1. Wykonaj następujące polecenie w wierszu poleceń:
   ```
   $ klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -
   svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
   ```
2. Uruchom ponownie usługę Serwer administracyjny Kaspersky Security Center, wykonując następujące polecenie:
   ```
   $ sudo systemctl restart kladminserver_srv
   ```

Port 13291 jest otwarty.

Aby sprawdzić, czy port 13291 został pomyślnie otwarty:

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)true
```

Wartość `true` oznacza, że port jest otwarty. W przeciwnym razie wyświetlana jest wartość `false`.

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 Linux 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 i modułów oprogramowania 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 firmy Kaspersky poprzez Kaspersky Security Center 14 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: Tworzenie zadania pobierania aktualizacji 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.

   Jak to zrobić: 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.

5. **Optymalizacja procesu aktualizacji przy użyciu plików diff (opcjonalnie)**

   Możesz zoptymalizować ruch pomiędzy 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

6. **Konfigurowanie automatycznej instalacji uaktualnień dla aplikacji zabezpieczających**

   Utwórz zadania *Aktualizacja* dla zarządzanych aplikacji, aby zapewnić najnowsze aktualizacje aplikacji, modułów oprogramowania i baz danych Kaspersky, w tym antywirusowych baz danych. Aby zapewnić dostarczanie aktualizacji na czas, zalecane jest włączenie opcji **Po pobraniu nowych uaktualnień do repozytorium** podczas konfigurowania terminarza zadania.

   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 13.2 oraz Agent sieciowy w wersji 13.2.

Jeśli aktualizacja wymaga przejrzenia i zaakceptowania warunków Umowy licencyjnej, następnie musisz najpierw zaakceptować warunki. Dopiero wtedy aktualizacja będzie mogła zostać przesłana na zarządzane urządzenia.

Wyniki

Po zakończeniu scenariusza Kaspersky Security Center Linux jest skonfigurowany do aktualizowania baz danych Kaspersky po pobraniu aktualizacji do repozytorium Serwera administracyjnego. 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 publicznego DNS. Jest to konieczne, aby zapewnić aktualizację antywirusowych baz danych oraz zachować poziom bezpieczeństwa zarządzanych urządzeń.

- Zainstalowane aplikacje firmy Kaspersky, w tym komponenty Kaspersky Security Center i aplikacje zabezpieczające

  Kaspersky Security Center nie może automatycznie aktualizować aplikacji Kaspersky. Aby zaktualizować aplikacje, pobierz najnowsze wersje aplikacji z witryny internetowej Kaspersky i zainstaluj je ręcznie:

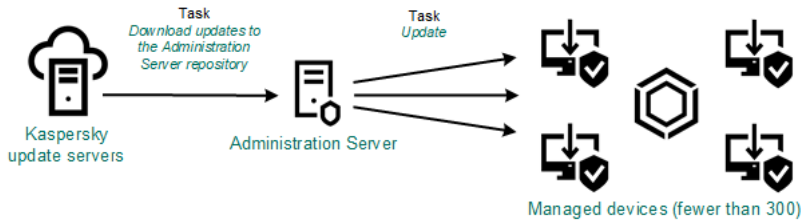
  - Serwer administracyjny Kaspersky Security Center, Kaspersky Security Center 14 Web Console
  - Agent sieciowy, Kaspersky Endpoint Security for Linux, sieciowa wtyczka administracyjna

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 for Linux 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).



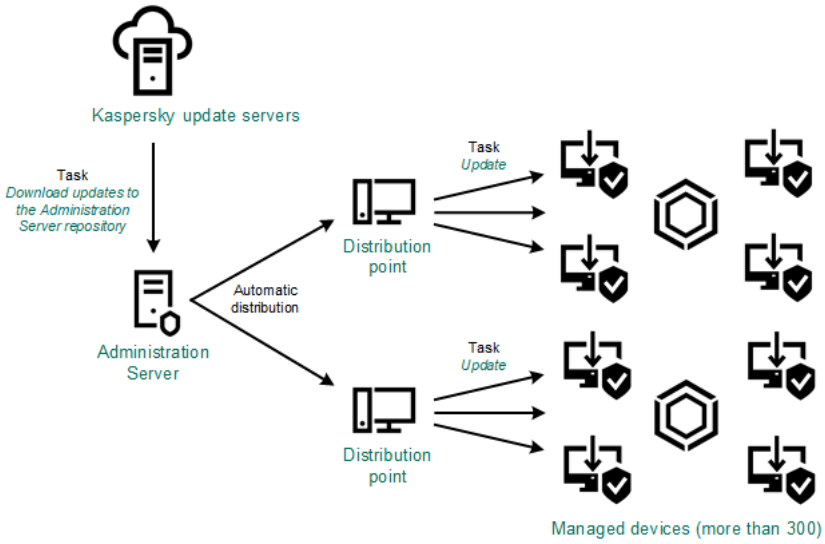
Aktualizowanie przy użyciu zadania Pobierz aktualizacje do repozytorium Serwera administracyjnego bez punktów dystrybucji

Jako źródło aktualizacji możesz użyć nie tylko serwerów aktualizacji Kaspersky, ale także folderu lokalnego lub sieciowego.

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 300 zarządzanych urządzeń lub więcej 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

Po zakończeniu zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* aktualizacje baz danych Kaspersky i modułów oprogramowania dla Kaspersky Endpoint Security for Linux są pobierane do repozytorium Serwera administracyjnego. Te aktualizacje są instalowane poprzez zadanie Aktualizacja dla Kaspersky Endpoint Security for Linux.

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.

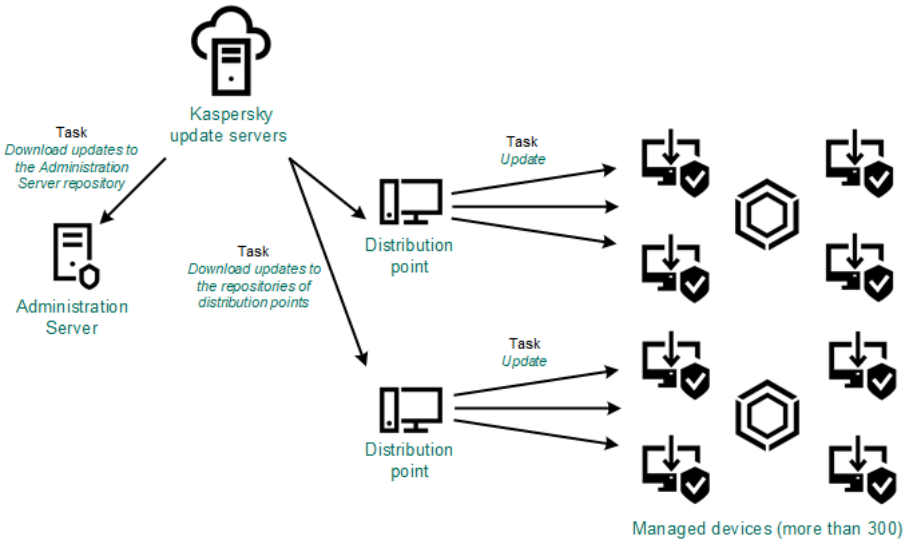
Każda aplikacja Kaspersky żąda wymaganych aktualizacji z Serwera administracyjnego. Serwer administracyjny gromadzi te żądania i pobiera tylko te uaktualnienia, które zostały zażądane przez aplikację. Dzięki temu te same uaktualnienia nie są pobierane kilka razy, a niepotrzebne uaktualnienia nie są pobierane 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

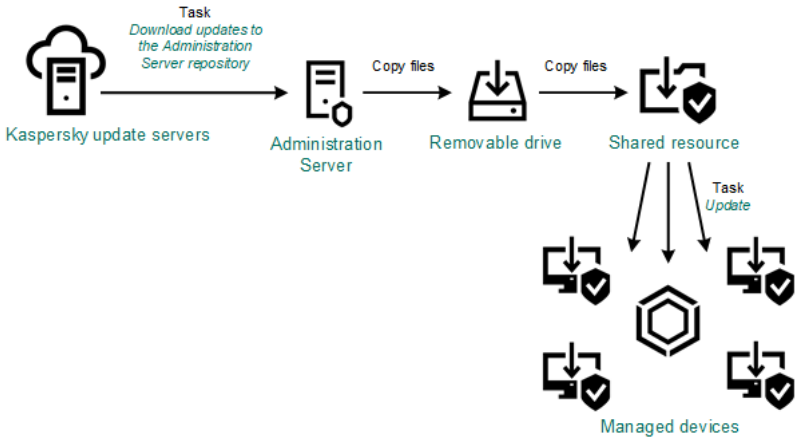
Domyślnie, Serwer administracyjny i punkty dystrybucji komunikują się z serwerami aktualizacji Kaspersky i pobierają uaktualnienia, korzystając z protokołu HTTPS. Możesz skonfigurować Serwer administracyjny i/lub punkty dystrybucji do używania protokołu HTTP zamiast HTTPS.

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.

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

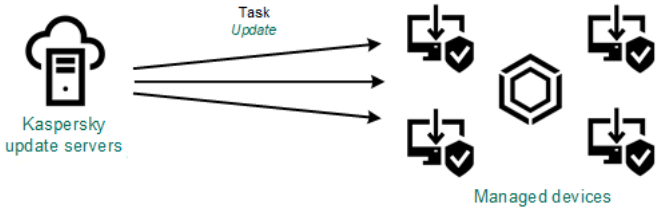
Jeśli urządzenia klienckie nie mają połączenia z Serwerem administracyjnym, możesz użyć folderu lokalnego lub zasobu współdzielonego jako źródła dla aktualizacji baz danych, modułów i aplikacji Kaspersky. W tym schemacie musisz skopiować wymagane aktualizacje z repozytorium Serwera administracyjnego na dysk wymienny, a następnie skopiować aktualizacje do folderu lokalnego lub zasobu współdzielonego, określonego jako źródło aktualizacji w ustawieniach Kaspersky Endpoint Security for Linux (patrz rysunek poniżej).



Aktualizowanie poprzez folder lokalny, folder współdzielony lub serwer FTP

Bezpośrednio z serwerów aktualizacji Kaspersky do Kaspersky Endpoint Security for Linux na zarządzanych urządzeniach

Na zarządzanych urządzeniach możesz skonfigurować Kaspersky Endpoint Security for Linux 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 repozytoria dostarczonegp przez Kaspersky Security Center. Aby pobierać aktualizacje bezpośrednio z serwerów aktualizacji Kaspersky, określ serwery aktualizacji Kaspersky jako źródło aktualizacji w aplikacji zabezpieczającej. Pełny opis tych ustawień można znaleźć w dokumentacji do Kaspersky Endpoint Security for Linux.

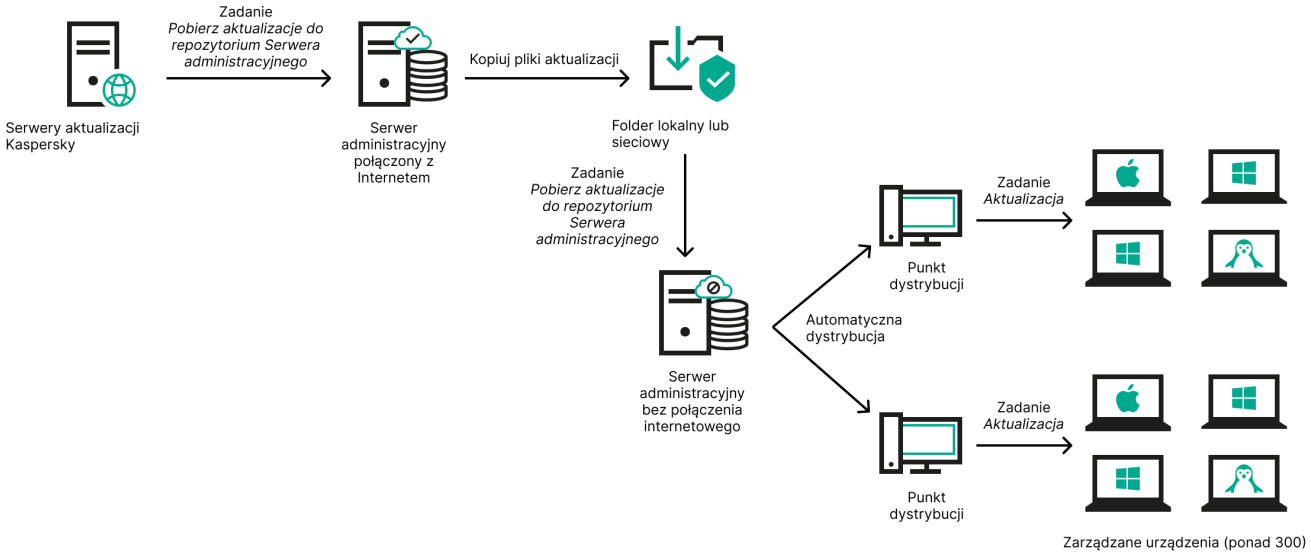
Poprzez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

Jeżeli Serwer administracyjny nie ma połączenia z Internetem, możesz skonfigurować zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, aby pobierać uaktualnienia z folderu lokalnego lub sieciowego. W takim przypadku należy od czasu do czasu kopiować wymagane pliki aktualizacji do określonego folderu. Na przykład możesz skopiować wymagane pliki aktualizacji z jednego z następujących źródeł:

- Serwer administracyjny z połączeniem internetowym (patrz rysunek poniżej)

  Ponieważ serwer administracyjny pobiera tylko aktualizacje wymagane przez aplikacje zabezpieczające, zestawy aplikacji zabezpieczających zarządzanych przez serwery administracyjne — ten, który ma połączenie z Internetem i ten, który go nie ma — muszą być zgodne.

  Jeżeli Serwer administracyjny, którego używasz do pobierania uaktualnień, ma wersję 13.2 lub wcześniejszą, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję **Pobierz aktualizacje za pomocą starego schematu**.



Aktualizacja przez folder lokalny lub sieciowy, jeśli Serwer administracyjny nie ma połączenia z Internetem

- Kaspersky Update Utility

  Ponieważ narzędzie to wykorzystuje stary schemat do pobierania uaktualnień, otwórz właściwości zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego*, a następnie włącz opcję *Pobierz aktualizacje za pomocą starego schematu*.

Tworzenie zadania Pobierz aktualizacje do repozytorium serwera administracyjnego.

Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* umożliwia pobieranie aktualizacji baz danych i modułów oprogramowania dla aplikacji zabezpieczających Kaspersky z serwerów aktualizacji Kaspersky do repozytorium Serwera administracyjnego.

Kreator szybkiego startu Kaspersky Security Center automatycznie tworzy zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* Serwera administracyjnego. Na liście zadań może znajdować się tylko jedno zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*. Możesz ponownie utworzyć to zadanie, jeśli zostanie usunięte z listy zadań Serwera administracyjnego.

Po zakończeniu zadania *Pobierz aktualizacje do repozytorium Serwera administracyjnego* i pobraniu aktualizacji można je rozprzestrzenić na zarządzane urządzenia.

Przed dystrybucją aktualizacji do urządzeń zarządzanych możesz uruchomić zadanie *Weryfikacja aktualizacji*. Pozwala to upewnić się, że Serwer administracyjny poprawnie zainstaluje pobrane aktualizacje, a poziom bezpieczeństwa nie zostanie obniżony 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. 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. 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.
6. Kliknij przycisk **Zakończ**.

   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 źródło aktualizacji możesz użyć serwerów aktualizacji Kaspersky, folderu lokalnego lub sieciowego albo głównego serwera administracyjnego.

   - **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.

   - **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.

- **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 (zaznaczone domyślnie)

    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 w celu zapewnienia wstecznej kompatybilności Kaspersky Security Center Linux.

    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 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.

- Dodatkowe ustawienia zadań:

  - **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, jeśli 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.

Wyświetlanie pobranych uaktualnień

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. Pobrane aktualizacje można wyświetlić w sekcji **AKTUALIZACJE BAZ DANYCH I MODUŁÓW OPROGRAMOWANIA KASPERSKY**.

W celu wyświetlenia listy pobranych uaktualnień:

W menu głównym przejdź do **OPERACJE → APLIKACJE KASPERSKY → AKTUALIZACJE BAZ DANYCH I MODUŁÓW OPROGRAMOWANIA KASPERSKY**.

Zostanie wyświetlona lista dostępnych aktualizacji.

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 antywirusowego dla aplikacji obsługiwanej przez Kaspersky Security Center, na przykład Kaspersky Endpoint Security for Linux. Podczas tworzenia zadań aktualizacji i skanowania antywirusowego określ grupę administracyjną z urządzeniami testowymi.

Zadanie *weryfikacji uaktualnień* uruchamia kolejno zadania aktualizacji i skanowania antywirusowego na urządzeniach testowych, aby sprawdzić, czy wszystkie aktualizacje są prawidłowe. Ponadto podczas tworzenia zadania *Weryfikacja uaktualnień* musisz określić zadania aktualizacji i skanowania antywirusowego.

3. Utwórz zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego*.

W celu skonfigurowania Kaspersky Security Center Linux 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 dodawania 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 antywirusowego.

      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 pobierania uaktualnień do repozytoriów punktów dystrybucji

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 dodawania zadań. 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.

Jeśli włączysz opcję **Nie używaj serwera proxy** dla źródeł aktualizacji Serwery aktualizacji Kaspersky lub Folder lokalny lub sieciowy, punkt dystrybucji nie będzie używać serwera proxy do pobierania aktualizacji, nawet jeśli włączono opcję **Użyj serwera proxy** w ustawieniach zasad agenta sieciowego dla punktu dystrybucji.

- **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** (zaznaczone domyślnie)

    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 w celu zapewnienia wstecznej kompatybilności Kaspersky Security Center Linux.

  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.

- 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.

Dodawanie źródeł uaktualnień dla zadania Pobierz uaktualnienia do repozytorium Serwera administracyjnego

Podczas tworzenia lub używania zadania pobierania uaktualnień do repozytorium Serwera administracyjnego możesz wybrać następujące źródła uaktualnień:

- Serwery aktualizacji Kaspersky
- Główny Serwer administracyjny

  Ten zasób dotyczy zadań utworzonych dla podrzędnego lub wirtualnego Serwera administracyjnego.
- Folder lokalny lub sieciowy

Serwery aktualizacji Kaspersky są używane domyślnie, ale aktualizacje można również pobierać z folderu lokalnego lub sieciowego. Możesz chcieć użyć tego folderu, jeśli Twoja sieć nie ma dostępu do Internetu. W takim przypadku możesz ręcznie pobrać aktualizacje z serwerów aktualizacji Kaspersky i umieścić pobrane pliki w odpowiednim folderze.

Możesz określić tylko jedną ścieżkę do folderu lokalnego lub sieciowego. Jako folder lokalny możesz używać tylko folderu na Serwerze administracyjnym; jako folder sieciowy możesz używać tylko serwera FTP lub HTTP.

Jeśli dodasz oba serwery aktualizacji Kaspersky oraz folder lokalny lub sieciowy, aktualizacje będą pobierane najpierw z folderu. W przypadku błędu podczas pobierania zostaną użyte serwery 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.

Aby dodać źródła aktualizacji:

1. Przejdź do **URZĄDZENIA→ ZADANIA**.

2. Kliknij **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
3. Przejdź do zakładki **Ustawienia aplikacji**.
4. W wierszu **Źródła aktualizacji** kliknij przycisk **Konfiguruj**.
5. W otwartym oknie kliknij przycisk **Dodaj**.
6. Na liście źródeł aktualizacji dodaj niezbędne źródła. Jeśli zaznaczysz pole wyboru **Folder lokalny lub sieciowy**, określ ścieżkę do folderu.
7. Kliknij przycisk **OK**, a następnie zamknij okno właściwości źródła uaktualnień.
8. W oknie zaktualizuj źródło kliknij przycisk **OK**.
9. Kliknij przycisk **Zapisz** w oknie zadania.

Teraz aktualizacje są pobierane do repozytorium Serwera administracyjnego z określonych źródeł.

Informacje o używaniu plików diff do aktualizowania baz danych i modułów aplikacji Kaspersky

Jeśli Kaspersky Security Center Linux 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.

Punkty dystrybucji nie używają multiemisji IP do automatycznego rozsyłania plików diff.

Włączania funkcji Pobierz pliki diff: scenariusz

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 tę funkcję w ustawieniach profilu Agenta sieciowego dla punktu dystrybucji, który otrzymuje aktualizacje z Serwera administracyjnego.

   Następnie włącz funkcję dla punktu dystrybucji, który pobiera uaktualnienia z Serwera administracyjnego.

   Funkcja jest włączona w ustawieniach polityki Agenta sieciowego i — jeśli punkty dystrybucji są przypisywane ręcznie i jeśli chcesz zastąpić ustawienia polityki — 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.

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 oknie głównym 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, przez który aktualizacje będą dostarczane na urządzenia klienckie w grupie.

4. W oknie właściwości punktu dystrybucji wybierz sekcję **Źródło aktualizacji**.

5. Wskaż źródło uaktualnień 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 dodawania zadań. Postępuj zgodnie z instrukcjami Kreatora.

   - **Pobierz pliki diff**

Ta opcja włącza funkcję pobierania plików diff.

Domyślnie opcja ta jest włączona.

Punkt dystrybucji będzie pobierał uaktualnienia z określonego źródła.

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.

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 odbierania 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 Kaspersky Endpoint Security for Linux, aby odbierała aktualizacje 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 Linux.

Po zakończeniu zadania aktualizacji, bazy danych i moduły Kaspersky są aktualne na urządzeniu.

Dostosowanie punktów dystrybucji i bram połączenia

Struktura grup administracyjnych w Kaspersky Security Center Linux pełni następujące funkcje:

- Tworzy zakres zasad

  Istnieje alternatywny sposób stosowania odpowiednich ustawień na urządzeniach przy użyciu *profili zasad*.

- 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.

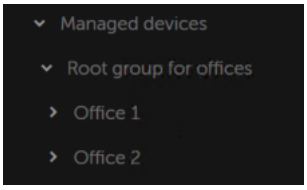
- Tworzenie struktury grup administracyjnych bez uwzględnienia topologii sieci. W tym przypadku należy wyłączyć automatyczne przydzielanie punktów dystrybucji, a następnie wskazać jedno lub kilka urządzeń jako

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 mają 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.

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 takim 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.

Automatyczne przypisywanie punktów dystrybucji

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center Linux sam wybierze urządzenia, które mają być punktami dystrybucji.

Aby automatycznie przypisać punkty dystrybucji:

1. W oknie głównym 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 Linux umożliwia ręczne wskazanie urządzeń do pełnienia roli punktów dystrybucji.

Zalecane jest automatyczne przypisywanie punktów dystrybucji. W tym przypadku, Kaspersky Security Center Linux 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 oknie głównym 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 wskaż nowo dodany punkt dystrybucji, aby otworzyć jego okno właściwości.

9. Skonfiguruj punkt dystrybucji w oknie właściwości:

- Sekcja **Ogólne** zawiera ustawienia interakcji pomiędzy punktem dystrybucji a urządzeniami klienckimi.

  - **Numer portu SSL**

    Numer portu SSL do nawiązywania zaszyfrowanych połączeń między urządzeniami klienckimi a punktem dystrybucji przy użyciu SSL.

    Domyślnie wykorzystywany jest port 13000.

  - **Użyj multicast**

    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 multicastu**

    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 Linux automatycznie przypisze unikatowy adres IP multiemisji w obrębie danego zakresu.

  - **Numer portu mulitcastu 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 uaktualnienia**

    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.

- W sekcji **Zakres** określ grupy administracyjne, do których punkt dystrybucji będzie dystrybuować aktualizacje.

- 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 dodawania zadań. Postępuj zgodnie z instrukcjami Kreatora.

  - **Pobierz pliki diff**

    Ta opcja włącza funkcję pobierania plików diff.

    Domyślnie opcja ta jest włączona.

- Skonfiguruj przeszukiwanie zakresów adresów IP przez punkt dystrybucji.

  - **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 **Włącz przeszukiwanie za pomocą technologii Zeroconf**, 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.

- 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. Przejdź do **URZĄDZENIA** → **Grupy**.
2. W strukturze grupy administracyjnej należy wybrać grupę administracyjną, dla której chcesz przejrzeć przypisane punkty dystrybucji.
3. Kliknij 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.

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. 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 Linux które dotyczą zarządzania aplikacjami firm trzecich uruchomionymi 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.

Komponent Kontrola aplikacji jest dostępny dla Kaspersky Endpoint Security 11.2 for Linux i nowszych wersji.

Wymagania wstępne

- Kaspersky Security Center Linux zostanie wdrożony w Twojej organizacji.
- Zasada Kaspersky Endpoint Security for Linux zostaje utworzona i jest aktywna.

Etapy

Scenariusz korzystania z Kontroli aplikacji podzielony jest na etapy:

1. **Tworzenie i przeglądanie listy plików wykonywalnych na urządzeniach klienckich**

   Ten etap pomaga w odnalezieniu plików wykonywalnych, które znajdują się na zarządzanych urządzeniach. Przejrzyj listę plików wykonywalnych i porównaj ją z listami dozwolonych i zabronionych plików wykonywalnych. Ograniczenia dotyczące użycia plików wykonywalnych mogą być związane z polityką bezpieczeństwa informacji, obowiązującej w Twojej organizacji. Możesz pominąć ten etap, jeśli wiesz dokładnie, jakie pliki wykonywalne są zainstalowane na zarządzanych urządzeniach.

   Jak to zrobić: Uzyskiwanie i przeglądanie listy plików wykonywalnych przechowywanych na urządzeniach klienckich

2. **Tworzenie kategorii aplikacji dla aplikacji używanych w Twojej organizacji**

   Przeanalizuj listy 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.

   Jak to zrobić: Tworzenie kategorii aplikacji z zawartością dodaną ręcznie

3. **Konfigurowanie Kontroli aplikacji w zasadzie Kaspersky Endpoint Security for Linux**

   Skonfiguruj komponent Kontrola aplikacji w zasadzie Kaspersky Endpoint Security for Linux, korzystając z kategorii aplikacji, które utworzono w poprzednim kroku.

4. **Weryfikowanie konfiguracji Kontroli aplikacji**

   Upewnij się, że wykonałeś następujące czynności:

   - Utworzyłeś kategorie aplikacji.

- Skonfigurowałeś Kontrolę aplikacji przy użyciu kategorii aplikacji.

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.

Szczegółowe informacje na temat Kontroli aplikacji znajdziesz w pomocy online Kaspersky Endpoint Security for Linux.

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 11.2 for Linux i nowszych wersji.

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 Linux możesz tworzyć tylko kategorie z zawartością dodaną ręcznie. Definiujesz warunki, na przykład, metadane plików, wartość skrótu pliku, certyfikat pliku, kategorię KL, ścieżkę do pliku, aby uwzględniać pliki wykonywalne w kategorii.

Szczegółowe informacje na temat Kontroli aplikacji znajdziesz w pomocy online Kaspersky Endpoint Security for Linux.

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 Kaspersky Endpoint Security 11.2 for Linux i nowszych wersji.

W celu utworzenia zadania dla plików wykonywalnych na urządzeniach klienckich:

1. 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 rozwijalnej **Aplikacja** wybierz Kaspersky Endpoint Security for Linux.

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 pomocy online Kaspersky Endpoint Security for Linux.

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:

Z listy rozwijalnej **OPERACJE → APLIKACJE INNYCH FIRM** wybierz **PLIKI WYKONYWALNE**.

Strona wyświetla listę plików wykonywalnych przechowywanych na urządzeniach klienckich.

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. Z listy rozwijalnej **OPERACJE → APLIKACJE INNYCH FIRM**wybierz **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**kreatora 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:

   - 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 Linux 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 for Linux obsługuje obliczenia SHA-256.

Wybierz jedną z opcji obliczania wartości sumy kontrolnej przez Kaspersky Security Center Linux dla plików w kategorii:

- Jeśli wszystkie instancje aplikacji zabezpieczających zainstalowane w Twojej sieci to Kaspersky Endpoint Security for Linux, zaznacz pole **SHA-256**.
- Zaznacz pole **Suma kontrolna MD5** tylko wtedy, gdy korzystasz z Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux nie obsługuje funkcji skrótu 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.

- Ze zarchiwizowanego folderu

Jeśli ta opcja jest zaznaczona, możesz określić plik zarchiwizowanego folderu, a następnie wybrać warunek, którego chcesz użyć do dodania aplikacji do kategorii użytkownika. Zarchiwizowany folder zostanie rozpakowany, a wybrane warunki zostaną zastosowane do plików w folderze. Jako warunek możesz wybrać jedno z następujących kryteriów:

- **Suma kontrolna pliku**

  Wybierz funkcję skrótu (MD5 lub SHA-256), której chcesz użyć do obliczenia wartości skrótu. Aplikacje, które mają tę samą wartość kontrolną co pliki w zarchiwizowanym folderze, zostaną dodane do kategorii aplikacji użytkownika.

  Wybierz funkcję skrótu MD5 tylko wtedy, gdy korzystasz z Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux nie obsługuje funkcji skrótu MD5.

- **Metadane**

  Ty wybierasz, których metadanych chcesz użyć jako kryteriów. Pliki wykonywalne, które zawierają te same metadane, zostaną dodane do kategorii użytkownika.

- **Certyfikat**

  Wybierz właściwości certyfikatu (podmiot certyfikatu, odcisk palca lub wystawca), których chcesz użyć jako kryteriów. Pliki wykonywalne, które zostały podpisane certyfikatami o tych samych właściwościach, zostaną dodane do kategorii użytkownika.

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.

Szczegółowe informacje na temat Kontroli aplikacji znajdziesz w pomocy online Kaspersky Endpoint Security for Linux.

Przeglądanie listy kategorii aplikacji

Możesz przejrzeć listę konfigurowanych kategorii aplikacji i ustawień każdej kategorii aplikacji.

W celu przejrzenia listy kategorii aplikacji:

Na zakładce **OPERACJE**, z listy rozwijalnej **APLIKACJE INNYCH FIRM** wybierz **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.

Dodawanie plików wykonywalnych dotyczących zdarzeń do kategorii aplikacji

Po skonfigurowaniu Kontroli aplikacji w zasadach Kaspersky Endpoint Security for Linux, 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. Przejdź do **MONITOROWANIE I RAPORTY → 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 **Dalej**.

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)**

  Wybierz tę opcję tylko wtedy, gdy korzystasz z Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux nie obsługuje funkcji skrótu MD5.

  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.

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.

Szczegółowe informacje na temat Kontroli aplikacji znajdziesz w pomocy online Kaspersky Endpoint Security for Linux.

Monitorowanie i raportowanie

W tej sekcji opisano możliwości monitorowania i raportowania Kaspersky Security Center Linux. Te możliwości dają ogląd infrastruktury, stanów ochrony i statystyk.

Po wdrożeniu Kaspersky Security Center Linux 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 Linux.

Wymagania wstępne

Po wdrożeniu Kaspersky Security Center Linux w sieci organizacji, możesz uruchomić jej monitorowanie i generować 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. **Wykonywanie zalecanych działań dla powiadomień krytycznych i ostrzegających**

   Dostępne instrukcje:

   Wykonaj zalecane działania dla sieci w swojej organizacji

4. **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

5. **Lokalizowanie urządzeń klienckich, które nie są chronione**

   Dostępne instrukcje:

- Przejrzyj widżet Nowe urządzenia
- Wygeneruj i przeczytaj Raport wdrażania ochrony

6. **Sprawdzanie ochrony urządzeń klienckich**

   Dostępne instrukcje:

   - Wygeneruj i sprawdź raporty z kategorii Stan ochrony i Statystyki zagrożeń
   - Uruchom i sprawdź wybór zdarzeń Krytyczny

7. **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:

   - Ograniczanie maksymalnej liczby zdarzeń

8. **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 14 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 14 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 14 Web Console, w sekcji **MONITOROWANIE I RAPORTY**, 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 14 Web Console posiada 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 RAPORTY → 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 RAPORTY → 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 RAPORTY** → **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 RAPORTY** → **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 RAPORTY → 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 RAPORTY → 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 14 Web Console, w sekcji **MONITOROWANIE I RAPORTY**, po kliknięciu **RAPORTY**.

Domyślnie, raporty zawierają informacje dla ostatnich 30 dni.

Kaspersky Security Center Linux zawiera 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 RAPORTY** → **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. W kroku **Okres raportowania** 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 RAPORTY** → **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. Kliknij przycisk **Zamknij** (⨯), aby zamknąć okno **Edytowanie raportu <Nazwa raportu>**.

Zaktualizowany szablon raportu pojawi się na liście szablonów raportu.

Eksportowanie raportu do pliku

Możesz wyeksportować raport do pliku XML lub HTML.

W celu wyeksportowania raportu do pliku:

1. Przejdź to **MONITOROWANIE I RAPORTY** → **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.

   Do konwersji raportu do formatu PDF wymagane jest narzędzie wkhtmltopdf. Po wybraniu opcji PDF Serwer administracyjny sprawdza, czy na urządzeniu jest zainstalowane narzędzie wkhtmltopdf. Jeżeli narzędzie nie jest zainstalowane, aplikacja wyświetla komunikat o konieczności zainstalowania narzędzia na urządzeniu Serwera administracyjnego. Zainstaluj narzędzie ręcznie, a następnie przejdź do następnego kroku.
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 RAPORTY** → **RAPORTY**.
2. Kliknij nazwę szablonu raportu, którego chcesz użyć do utworzenia raportu.

Raport zostanie wygenerowany przy użyciu wybranego szablonu i wyświetlony.

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. Przejdź to **MONITOROWANIE I RAPORTY** → **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.

      Do konwersji raportu do formatu PDF wymagane jest narzędzie wkhtmltopdf. Po wybraniu opcji PDF Serwer administracyjny sprawdza, czy na urządzeniu jest zainstalowane narzędzie wkhtmltopdf. Jeżeli narzędzie nie jest zainstalowane, aplikacja wyświetla komunikat o konieczności zainstalowania narzędzia na urządzeniu Serwera administracyjnego. Zainstaluj narzędzie ręcznie, a następnie przejdź do następnego kroku.

   c. Czy raporty są wysyłane za pośrednictwem poczty elektronicznej wraz z ustawieniami powiadomień e-mail.
   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, w kroku **Zakończ tworzenie zadania** 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 RAPORTY** → **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 Linux 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 14 Web Console.

Wybory zdarzeń są dostępne w Kaspersky Security Center 14 Web Console, w sekcji **MONITOROWANIE I RAPORTY**, po kliknięciu **WYBORY ZDARZEŃ**.

Domyślnie, wybory zdarzeń zawierają informacje dla ostatnich siedmiu dni.

Kaspersky Security Center Linux zawiera 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 Linux 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 RAPORTY → 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 RAPORTY → 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 RAPORTY → 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 RAPORTY → 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 Linux 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. Wybierz **URZĄDZENIA → ZASADY I PROFILE**.
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 górnej części ekranu 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 Linux, 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 Linux posiada swój zestaw typów zdarzeń. W tej sekcji wymienione są typy zdarzeń, które występują w Serwerze administracyjnym Kaspersky Security Center Linux i Agencie sieciowym. 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 Linux, 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 Linux, 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 okres przechowywania zdarzeń: Ustawianie okresu przechowywania zdarzenia

Zdarzenia Serwera administracyjnego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Serwera administracyjnego.

Zdarzenia krytyczne Serwera administracyjnego

Poniższa tabela przedstawia zdarzenia serwera administracyjnego Kaspersky Security Center Linux, które mają priorytet **Krytyczny**.

Zdarzenia krytyczne Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Domyśln przechow
Limit licencji został przekroczony	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Raz dziennie Kaspersky Security Center Linux sprawdza, czy ograniczenia licencyjne nie są przekroczone.	180 dni

			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 Linux określa reguły generowania zdarzeń, gdy ograniczenia licencjonowania zostaną przekroczone.	
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 dni

			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 dni
Plik klucza został dodany do listy zablokowanych	4124	KLSRV_LICENSE_BLACKLISTED	Zdarzenia tego typu występują, gdy firma Kaspersky dodała kod aktywacyjny lub plik klucza, którego używasz, do listy blokowanych. Aby uzyskać więcej informacji, skontaktuj się z działem pomocy technicznej.	180 dni
Licencja wkrótce utraci ważność	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Tego typu zdarzenia mają miejsce, gdy zbliża się data wygaśnięcia licencji komercyjnej.	180 dni

			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. Tej liczby dni nie można zmienić. 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 Linux zapewnia tylko podstawową funkcjonalność. Możesz zareagować na zdarzenie w następujące sposoby: • Upewnij się, że zapasowy klucz licencyjny został dodany do Serwera administracyjnego. • Jeśli korzystasz z subskrypcji, pamiętaj o jej odnowieniu. Nieograniczona subskrypcja jest odnawiana automatycznie, jeśli została opłacona w odpowiednim terminie.	
Certyfikat wygasł	4132	KLSRV_CERTIFICATE_EXPIRED	Zdarzenia tego typu występują, gdy certyfikat Serwera administracyjnego dla Zarządzania urządzeniami mobilnymi utraci ważność.	180 dni

			Należy zaktualizować certyfikat, który utracił ważność. Możesz skonfigurować automatyczne aktualizacje certyfikatów, zaznaczając pole **Odnów certyfikat automatycznie, jeśli jest to możliwe** w ustawieniach wydawania certyfikatów.	

Zdarzenia błędu funkcyjnego Serwera administracyjnego

Poniższa tabela wyświetla zdarzenia Kaspersky Security Center Linux Administration Server, które posiadają priorytet **Błąd funkcjonalny**.

Zdarzenia błędu funkcyjnego Serwera administracyjnego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Opis	Dor prze
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
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 Linux 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:	180

			• 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.	
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 zaktualizować bazy danych i moduły oprogramowania, postępuj zgodnie z instrukcjami.	180
Brak wolnego miejsca na dysku	4107	KLSRV_DISK_FULL	Tego typu zdarzenia występują, gdy dysk	180

			twardy urządzenia, na którym jest zainstalowany Serwer administracyjny, zabraknie wolnego miejsca. Zwolnij miejsce na dysku na urządzeniu.	
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
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	180

			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: • 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	180

			ustawienia zasady Kaspersky Endpoint Security for Linux 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. Sprawdzenie informacji dotyczących wyboru systemu DBMS.	

Zdarzenia ostrzegające Serwera administracyjnego

Poniższa tabela przedstawia zdarzenia Serwera administracyjnego Kaspersky Security Center Linux Administration Server o priorytecie **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 Linux sprawdza, czy ograniczenia licencyjne nie są przekroczone.	90 d

			Zdarzenia tego typu występują, gdy Serwer administracyjny wykryje, że niektóre ograniczenia licencyjne są przekroczone przez aplikacje firmy Kaspersky zainstalowane na urządzeniach klienckich i czy liczba aktualnie używanych jednostek licencyjnych objętych jedną licencją stanowi od 100% do 110% całkowitej liczby jednostek objętych licencją. Nawet jeśli to zdarzenie wystąpi, urządzenia klienckie są chronione. Możesz zareagować na zdarzenie w następujące sposoby: • Zapoznaj się z listą zarządzanych urządzeń. Usuń urządzenia, które nie są w użyciu. • Dostarcz licencję dla większej liczby urządzeń (dodaj ważny kod aktywacyjny lub plik klucza do Serwera administracyjnego). Kaspersky Security Center Linux 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.	90 d

			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 Kaspersky Security Center 14 Web Console. • Określ przedział czasu, po którym urządzenie zostanie automatycznie usunięte z grupy, przy użyciu Kaspersky Security Center 14 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.	90 d

			Aby uniknąć tego problemu, przełącz Agenta sieciowego do trybu klonowania dysku na odpowiednim urządzeniu przed sklonowaniem dysku twardego tego urządzenia.	
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 firm trzecich, 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	90 c

			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 wydawanie zostało zainicjowane dla certyfikatu, dla którego wyłączona jest opcja **Odnów certyfikat automatycznie, jeśli jest to możliwe**. Może to być spowodowane błędem, który wystąpił podczas tworzenia certyfikatu. Konieczne może być ręczne ponowne wystawienie certyfikatu. • Jeśli korzystasz z integracji z infrastrukturą klucza publicznego, przyczyną może być brak atrybutu SAM-Account-Name konta użytego do integracji z PKI oraz do wydania certyfikatu.	90 c

			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 d
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 j 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 j prze
Błąd podczas	4138	KLSRV_GCM_DEVICE_ERROR	Zdarzenia tego typu	90 d

przesyłania wiadomości FCM do urządzenia mobilnego			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 serwer FCM nie może obsłużyć niektórych żądań otrzymanych z Serwera administracyjnego. To oznacza, że niektóre zarządzane urządzenia mobilne nie otrzymają powiadomienia push. Przeczytaj kod Http w szczegółach opisu zdarzenia i zareaguj odpowiednio. Więcej informacji na temat kodów HTTP otrzymanych z 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 serwer FCM zwróci żądanie do Serwera administracyjnego z kodem HTTP innym niż 200 (OK).	90 c

			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 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.	90 c

			Jeżeli nie znajdziesz rozwiązania swojego problemu, skontaktuj się z działem pomocy technicznej firmy Kaspersky.	
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 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.	90 c

			• 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 Linux 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. Sprawdzenie 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.	90 c

			Przeczytaj dziennik zdarzeń aplikacji Kaspersky na urządzeniu, na którym jest zainstalowany podrzędny Serwer administracyjny i zareaguj odpowiednio.	
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 c
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 Kaspersky Security Center Web Console.	90 c
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	Nie j prze

			przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	
Przekroczono limit wydarzeń w bazie danych. Usunięto wydarzenia	4146	KLSRV_EVP_DB_TRUNCATED	Zdarzenia tego typu występują, jeśli starsze zdarzenia zostały usunięte z bazy danych Serwera administracyjnego po osiągnięciu pojemności bazy danych Serwera administracyjnego. Możesz zareagować na zdarzenie w następujące sposoby: • Zmiana maksymalnej dozwolonej liczby zdarzeń przechowywanych w bazie danych Serwera administracyjnego. • Zmniejszenie listy zdarzeń przechowywanych w bazie danych Serwera administracyjnego.	Nie j prze

Zdarzenia informacyjne Serwera administracyjnego

Poniższa tabela przedstawia zdarzenia Serwera administracyjnego Kaspersky Security Center Linux Administration Server o priorytecie **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

Zdarzenia Agenta sieciowego

Ta sekcja zawiera informacje o zdarzeniach dotyczących Agenta sieciowego.

Zdarzenia ostrzegające Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center Linux, które posiadają priorytet **Ostrzeżenie**.

Zdarzenia ostrzegające Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
Wystąpił incydent	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dni

Zdarzenia informacyjne Agenta sieciowego

Poniższa tabela wyświetla zdarzenia Agenta sieciowego Kaspersky Security Center Linux, które posiadają priorytet **Informacja**.

Zdarzenia informacyjne Agenta sieciowego

Nazwa wyświetlanego typu zdarzenia	ID typu zdarzenia	Typ zdarzenia	Domyślny czas przechowywania
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
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

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 Linux, 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 oknie głównym 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 oknie głównym 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.

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.

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 Linux 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 RAPORTY → 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 RAPORTY → 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 RAPORTY → 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 konsoli Kaspersky Security Center 14 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 RAPORTY**.

Informacje o stanach urządzeń

Kaspersky Security Center Linux 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 Linux bierze pod uwagę flagę widoczności urządzenia w sieci (patrz tabela poniżej). Jeśli Kaspersky Security Center Linux nie znajdzie urządzenia w sieci w ciągu dwóch godzin, flaga widoczności urządzenia zostanie ustawiona na *Nie jest widoczne*.

Stany są następujące:

- *Krytyczny* lub *Krytyczny / Widoczny*
- *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 skanowania antywirusowego 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 antywirusowe nie było wykonywane od dłuższego czasu	Urządzenie jest widoczne w sieci, a aplikacja zabezpieczająca jest zainstalowana na urządzeniu, ale zadanie Skanowanie antywirusowe 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.
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.
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 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 Linux 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 Linux z poprzedniej wersji, wartości warunku **Bazy danych są nieaktualne** dla przypisania stanu do *Krytyczne* lub *Ostrzeżenie* nie zmienią się.

Jeśli Kaspersky Security Center Linux 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 Linux. W zależności od wybranej metody powiadamiania, dostępne są następujące typy powiadomień:

- E-mail — Po wystąpieniu zdarzenia, Kaspersky Security Center Linux wyśle powiadomienie na określone adresy e-mail.
- SMS — Po wystąpieniu zdarzenia, Kaspersky Security Center Linux 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 Linux:

1. W górnej części ekranu kliknij ikonę **Ustawienia** () obok nazwy żądanego Serwera administracyjnego.

   Okno właściwości Serwera administracyjnego zostanie otwarte na wybranej 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 **Serwer SMTP** określ adresy serwera poczty e-mail, oddzielając je średnikami. Możesz użyć następujących wartości:

- Adres IPv4 lub IPv6
- 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 Linux sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center Linux 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.

Przycisk **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie na wskazany adres e-mail.

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 **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.

- SMS

Na zakładce **SMS** możesz skonfigurować wysyłanie powiadomień SMS o różnych zdarzeniach na telefon komórkowy. Wiadomości SMS zostaną wysłane 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 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 Linux sprawdza, czy certyfikat serwera SMTP jest również podpisany przez zaufane urzędy certyfikacji. Kaspersky Security Center Linux 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 **Wyślij wiadomość testową** umożliwia sprawdzenie, czy ustawienia powiadamiania zostały skonfigurowane poprawnie: aplikacja wyśle testowe powiadomienie do określonego odbiorcy.

Kliknięcie odnośnika **Ustaw limit liczby powiadomień** umożliwia zdefiniowanie maksymalnej liczby powiadomień, które aplikacja może wysłać w określonym przedziale czasu.

- **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 Linux.

Możesz zastąpić ustawienia dostarczania powiadomień dla pewnych zdarzeń w sekcji **Konfiguracja zdarzenia** ustawień Serwera administracyjnego, ustawień zasady lub ustawień aplikacji.

Sprawdzanie opcji wysyłania powiadomień

Aby sprawdzić, czy powiadomienia o zdarzeniach są dostarczane, aplikacja używa powiadomień o wykryciu na urządzeniach klienckich wirusa testowego EICAR.

W celu sprawdzenia opcji wysyłania powiadomień o zdarzeniach:

1. Zatrzymaj zadanie ochrony systemu plików w czasie rzeczywistym na urządzeniu klienckim, a następnie skopiuj na nie wirusa testowego EICAR. Następnie, 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.

Aby otworzyć zapis wykrycia wirusa testowego:

1. W menu głównym przejdź do **MONITOROWANIE I RAPORTY → WYBORY ZDARZEŃ**.
2. Kliknij nazwę wyboru **Ostatnie zdarzenia**.

   W oknie, które zostanie otwarte, wyświetlone zostanie powiadomienie o wirusie testowym.

Wirus testowy EICAR nie zawiera kodu, który mógłby zaszkodzić 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 Linux 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 Linux
%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 RAPORTY → 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 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. Domyślnie ogłoszenia Kaspersky są 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.

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 14 Web Console wyświetli etykietę powiadomienia odpowiadającą poziomowi istotności ogłoszeń. Możesz kliknąć etykietę, aby wyświetlić to ogłoszenie w sekcji Ogłoszenia firmy Kaspersky.

Możesz określić Ustawienia ogłoszeń firmy Kaspersky, w tym kategorie ogłoszeń, które chcesz przeglądać, i gdzie wyświetlać etykietę powiadomienia. Jeśli nie chcesz otrzymywać ogłoszeń, możesz wyłącz tę funkcję.

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 RAPORTY → 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 RAPORTY** i jego podsekcjach.

4. Kliknij przycisk **OK**.

   Zostaną określone ustawienia ogłoszeń firmy Kaspersky.

Wyłączanie ogłoszeń Kaspersky

Sekcja Ogłoszenia firmy Kaspersky (**MONITOROWANIE I RAPORTY → 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.

W celu wyłączenia ogłoszeń Kaspersky:

1. W oknie głównym aplikacji kliknij ikonę **ustawienia** ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na zakładce **Ogólne** wybierz sekcję **Ogłoszenia firmy Kaspersky**.

3. Przełącz przycisk przełączania na pozycję **Ogłoszenia związane z bezpieczeństwem są wyłączone**.

4. Kliknij przycisk **Zapisz**.

   Ogłoszenia firmy Kaspersky są wyłączone.

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 Linux umożliwia skonfigurowanie eksportu zdarzeń do systemów SIEM za pomocą jednej z następujących metod: eksport do dowolnego systemu SIEM używającego formatu Syslog lub eksport 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 Linux:

- 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 Linux**

  Instrukcja: Konfigurowanie eksportowania zdarzeń w systemie SIEM

- **Wybieranie zdarzeń, które chcesz wyeksportować do systemu SIEM**

  Zaznacz zdarzenia, które chcesz wyeksportować do systemu SIEM Najpierw zaznacz ogólne zdarzenia, które występują we wszystkich zarządzanych aplikacjach Kaspersky. Następnie możesz oznaczyć zdarzenia dla określonych zarządzanych aplikacji Kaspersky .

- **Konfiguracja eksportu zdarzeń do systemu SIEM**

  Można eksportować zdarzenia przy użyciu jednej z następujących metod:

  - Korzystanie z protokołów TCP/IP, UDP lub TLS przez protokoły TCP.
  - 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 wyniki eksportu, jeśli wybrano zdarzenia, które chcesz wyeksportować.

Czynności niezbędne do wykonania przed rozpoczęciem pracy

Podczas konfigurowania automatycznego eksportowania zdarzeń w Kaspersky Security Center Linux musisz określić niektóre ustawienia systemu SIEM. Zalecane jest wcześniejsze sprawdzenie tych ustawień w celu przygotowania do konfiguracji Kaspersky Security Center Linux .

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 Linux a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center Linux i w ustawieniach odbiornika Twojego systemu SIEM.

- **Protokół**

  Protokół używany do przesyłania wiadomości z Kaspersky Security Center Linux do Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center Linux i w ustawieniach odbiornika Twojego systemu SIEM.

Informacje o zdarzeniach w Kaspersky Security Center Linux

Kaspersky Security Center Linux 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 urządzeń.

Wydarzenia według typu

W Kaspersky Security Center Linux 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.

Wydarzenia według źródła

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.

Zdarzenia mogą być generowane przez następujące aplikacje:

- Składniki Kaspersky Security Center Linux:
  - Serwer administracyjny
  - Agent sieciowy
- Zarządzane aplikacje Kaspersky

  Szczegółowe informacje na temat zdarzeń generowanych przez aplikacje zarządzane przez Kaspersky można znaleźć w dokumentacji odpowiedniej aplikacji.

Zdarzenia według poziomu ważności

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 Linux. 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 Linux do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia – Kaspersky Security Center Linux oraz odbiorca zdarzenia – system SIEM. Aby pomyślnie eksportować zdarzenia, należy skonfigurować tę funkcję w posiadanym systemie SIEM i w Konsoli administracyjnej Kaspersky Security Center Linux. Nie ma znaczenia, która strona zostanie skonfigurowana jako pierwsza. Możesz skonfigurować przesyłanie zdarzeń w Kaspersky Security Center Linux, a następnie skonfigurować odbieranie zdarzeń przez system SIEM lub na odwrót.

Format Syslog eksportu zdarzeń

Możesz wysyłać zdarzenia w formacie Syslog do dowolnego systemu SIEM. Korzystając z formatu Syslog, możesz przekazywać wszelkie zdarzenia, które występują na Serwerze administracyjnym oraz w aplikacjach Kaspersky, które są zainstalowane na zarządzanych urządzeniach. Podczas eksportowania zdarzeń w formacie Syslog możesz wybrać dokładne typy zdarzeń, które będą przesyłane do systemu SIEM.

Odbieranie zdarzeń przez system SIEM

System SIEM musi odbierać i poprawnie analizować zdarzenia otrzymywane z Kaspersky Security Center Linux. 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 Linux do zewnętrznych systemów SIEM składa się na dwie części: nadawca zdarzenia – Kaspersky Security Center Linux oraz odbiorca zdarzenia – system SIEM. Należy skonfigurować eksportowanie zdarzeń w posiadanym systemie SIEM i w Kaspersky Security Center Linux.

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 Linux, należy skonfigurować odbiorcę w swoim systemie SIEM. W systemie SIEM powinny zostać określone następujące ustawienia:

- **Protokół eksportu**

  Protokół przesyłania komunikatów, UDP, TCP lub TLS, przez TCP. Ten protokół musi być taki sam, jak protokół, który określono w Kaspersky Security Center Linux.

- **Port**

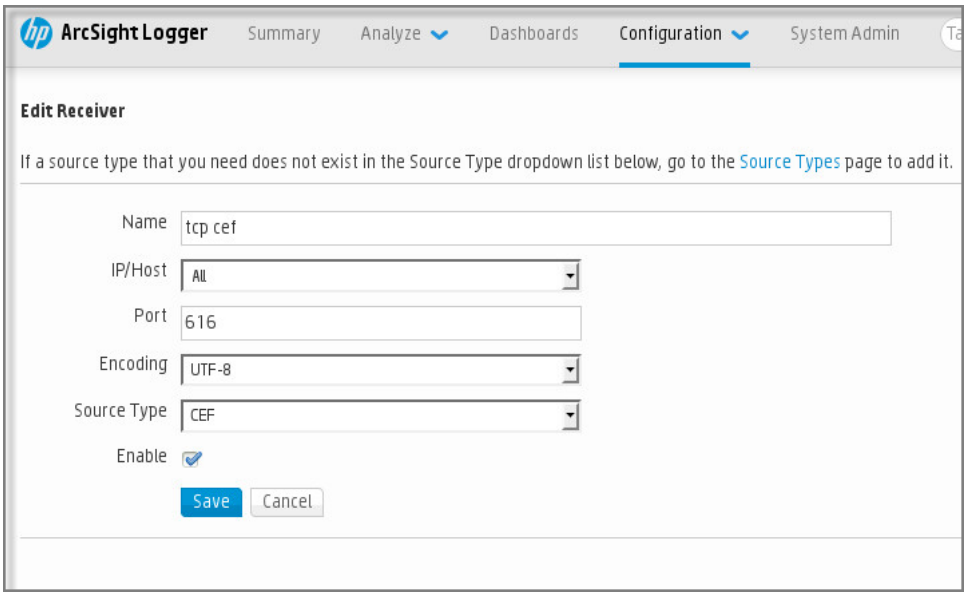
  Określ numer portu do nawiązana połączenia z Kaspersky Security Center Linux. Ten port musi być taki sam, jak port określony w Kaspersky Security Center Linux podczas konfiguracji z systemem SIEM.

- **Format danych**

  Określ format Syslog.

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 Linux 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 → ZASADY I PROFILE**.
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:

   - Kliknij ikonę **Ustawienia** (🔧) obok nazwy żądanego Serwera administracyjnego.
   - W menu głównym przejdź do **URZĄDZENIA** → **ZASADY I PROFILE**, 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 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 Linux do systemów zewnętrznych.

W Kaspersky Security Center Linux 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 Linux jest konfigurowany tak, aby wysyłał zdarzenia do systemu SIEM. Kaspersky Security Center Linux 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 Linux do wyeksportowania zdarzeń do systemu SIEM

Aby wyeksportować zdarzenia do systemu SIEM, musisz skonfigurować proces eksportu w Kaspersky Security Center Linux.

W celu skonfigurowania eksportowania do systemów SIEM w Kaspersky Security Center 14 Web Console:

1. Z listy rozwijalnej **Ustawienia konsoli** wybierz **Integracja**.

   Zostanie otwarte okno **Ustawienia konsoli**.

2. Wybierz zakładkę **Integracja**.

3. Na zakładce **Integracja** wybierz sekcję **SIEM**.

4. Kliknij odnośnik **Ustawienia**.

   Zostanie otwarta sekcja **Eksportuj ustawienia**.

5. 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 Linux a serwerem Twojego systemu SIEM. Tę wartość należy określić w ustawieniach Kaspersky Security Center Linux 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 Linux. Kaspersky Security Center Linux 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 Linux 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 Linux 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 Linux przechowuje wygenerowany certyfikat z podpisem własnym i możesz przekazać publiczną część certyfikatu lub odcisk palca SHA1 do systemu SIEM.

6. Jeśli chcesz, możesz wyeksportować zarchiwizowane zdarzenia z bazy danych Serwera administracyjnego i ustawić datę początkową, od której chcesz rozpocząć eksport zarchiwizowanych zdarzeń:

   a. Kliknij łącze **Wybierz datę rozpoczęcia eksportu** łącza.

   b. W otwartej sekcji określ datę rozpoczęcia w polu **Data rozpoczęcia eksportu od**.

   c. Kliknij przycisk **OK**.

7. Przełącz opcję na pozycję **Automatycznie eksportuj zdarzenia do bazy danych systemu SIEM WŁĄCZONO.**

8. Kliknij przycisk **Zapisz**.

Eksportowanie do systemu SIEM zostało skonfigurowane. Od teraz, jeśli skonfigurowano odbieranie zdarzeń w systemie SIEM, Serwer administracyjny eksportuje zaznaczone zdarzenia do systemu SIEM. Jeśli ustawisz datę rozpoczęcia eksportu, Serwer administracyjny wyeksportuje również zaznaczone zdarzenia przechowywane w bazie danych Serwera administracyjnego od określonej daty.

Eksportowanie zdarzeń bezpośrednio z bazy danych

Zdarzenia można otrzymywać bezpośrednio z bazy danych Kaspersky Security Center Linux bez konieczności korzystania z interfejsu Kaspersky Security Center Linux. 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 Linux 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 Linux, 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 Linux, 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. Jeśli tworzysz zapytanie SQL przy użyciu narzędzia klsql2, nie musisz wprowadzać nazwy bazy danych i parametrów dostępu, ponieważ zapytanie adresuje widoki publiczne Kaspersky Security Center Linux bezpośrednio.

W celu pobrania i użycia narzędzia klsql2:

1. Pobierz narzędzie klsql2 ze strony internetowej Kaspersky.
2. Skopiuj i rozpakuj pobrany plik klsql2.zip do dowolnego folderu na urządzeniu z zainstalowanym Serwerem administracyjnym Kaspersky Security Center Linux.

   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 Linux, 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 -o result.xml
   ```
6. Otwórz nowo utworzony plik result.xml, aby wyświetlić wyniki zapytania.

Możesz zmodyfikować plik src.sql i utworzyć dowolne zapytanie do widoków publicznych. Następnie, z poziomu wiersza poleceń, wykonaj zapytanie 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 Linux

Jeśli chcesz uzyskać dostęp do bazy danych Kaspersky Security Center Linux przy użyciu narzędzi do zarządzania serwerem SQL lub bazą danych MySQL lub MariaDB, musisz znać nazwę bazy danych, aby nawiązać z nią połączenie z poziomu swojego edytora skryptów SQL.

W celu wyświetlenia nazwy bazy danych Kaspersky Security Center Linux:

1. Kliknij ikonę **Ustawienia** ( ) obok nazwy żądanego Serwera administracyjnego.

   Zostanie otwarte okno właściwości Serwera administracyjnego.

2. Na karcie **Ogólne**, a następnie wybierz sekcję **Szczegóły bieżącej bazy danych**.

Nazwa bazy danych jest określona w polu **Nazwa bazy danych**. Użyj nazwy bazy danych, aby adresować bazę danych w swoich zapytaniach SQL.

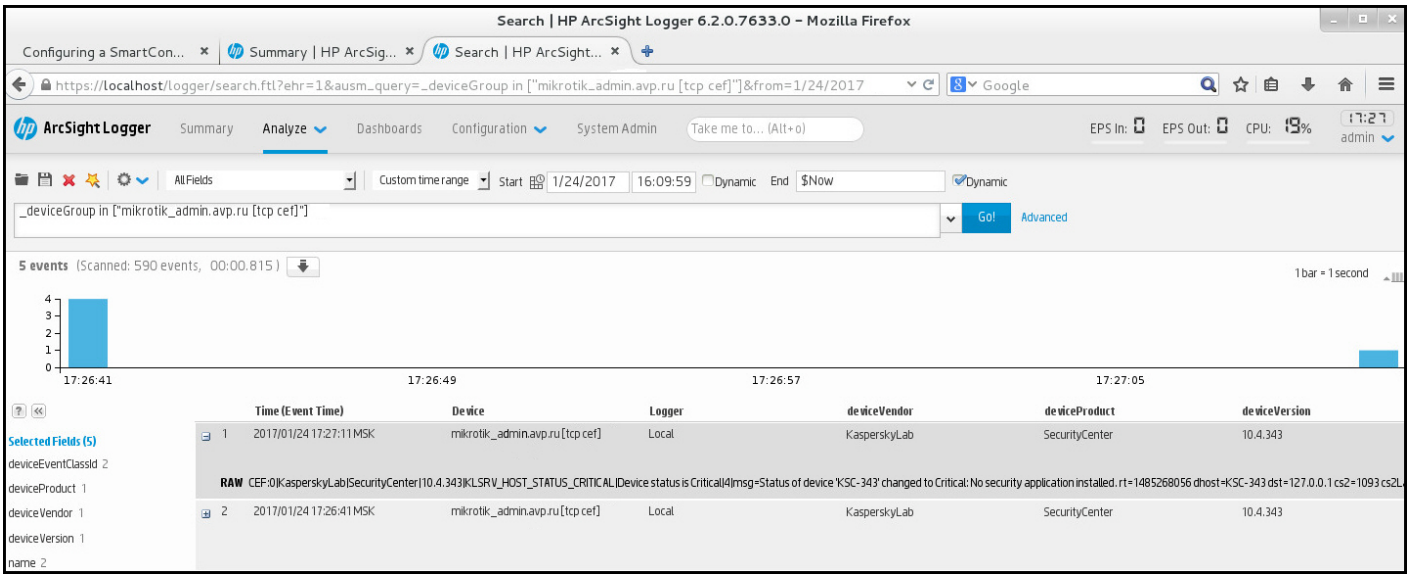
Przeglądanie wyników eksportowania

Możesz kontrolować pomyślne zakończenie procedury eksportowania zdarzeń. W tym celu sprawdź, czy wiadomości z eksportowanymi zdarzeniami są otrzymywane przez Twój system SIEM.

Jeśli zdarzenia wysłane z Kaspersky Security Center Linux są odbierane i poprawnie analizowane przez Twój system SIEM, konfiguracja po obu stronach została przeprowadzona właściwie. Jeśli jest inaczej, sprawdź ustawienia, które określono w Kaspersky Security Center Linux, 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

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. W menu głównym przejdź do sekcji **URZĄDZENIA → WYBORY URZĄDZEŃ** lub **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. Przejdź do **URZĄDZENIA** → **WYBORY URZĄDZEŃ** URZĄDZEŃ.

   Zostanie wyświetlona lista wyborów urządzeń.

2. Kliknij odpowiedni wybór urządzenia zdefiniowany przez użytkownika.

   Zostanie otwarte okno **Ustawienia wyboru urządzeń**.

3. Na zakładce **Ogólne** określ warunki, jakie muszą zostać spełnione do uwzględnienia urządzeń w tym wyborze.

4. Kliknij przycisk **Zapisz**.

Ustawienia zostaną zastosowane i zapisane.

Poniżej znajdują się opisy warunków przydzielania urządzeń do wyboru. Warunki są łączone przy użyciu operatora logicznego LUB: Wybór będzie zawierał urządzenia odpowiadające przynajmniej jednemu z wymienionych warunków.

Ogólne

W sekcji **Ogólne** możesz zmienić nazwę warunku wyboru oraz określić, czy ten warunek ma być odwrócony:

Odwróć warunek wyboru

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**
- Domena Windows

  Wyświetla wszystkie urządzenia znajdujące się w określonej w grupie roboczej.

- Grupa administracyjna

  Wyświetla urządzenia znajdujące się w określonej grupie administracyjnej.

- Opis

Tekst wyświetlany w oknie właściwości urządzenia: pole **Opis**sekcji **Ogólne**.

W celu opisania tekstu w polu **Opis** możesz użyć następujących znaków:

- W słowie:
  - *****. Zastępuje dowolny wiersz dowolną liczbą znaków.

    Na przykład:

    Aby opisać słowa **Serwer** lub **Serwera**, możesz wpisać **Serwer***.
  - **?.** Zastępuje dowolny pojedynczy znak.

    Na przykład:

    Aby opisać wyrażenia, takie jak **SUSE Linux Enterprise Server 12** lub **SUSE Linux Enterprise Server 15**, możesz wpisać **SUSE Linux Enterprise Server 1?**.

    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.

Aktywność sieciowa

W sekcji **Aktywność sieciowa** możesz określić kryteria, które będą używane do uwzględniania urządzeń w wyborze zgodnie z ich aktywnością sieciową:

- Urządzenie jest punktem dystrybucji

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

  - **Tak**. Wybór zawiera urządzenia pełniące role punktów dystrybucji.
  - **Nie**. Urządzenia pełniące role punktów dystrybucji nie będą uwzględniane w wyborze.
  - **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Nie odłączaj od Serwera administracyjnego

Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

- **Włączona**. Wybór będzie zawierał urządzenia, na których zaznaczono pole **Nie odłączaj od Serwera administracyjnego**.
- **Wyłączona**. Wybór będzie zawierał urządzenia, na których odznaczono pole **Nie odłączaj od Serwera administracyjnego**.
- **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Przełączanie profilu połączenia

Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

- **Tak**. Wybór będzie zawierał urządzenia, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
- **Nie**. Wybór nie będzie zawierał urządzeń, które zostały podłączone do Serwera administracyjnego po przełączeniu profilu połączenia.
- **Nie wybrano wartości**. Kryterium nie będzie stosowane.

- Ostatnie połączenie z Serwerem administracyjnym

To pole ustawia kryterium wyszukiwania urządzeń według godziny ostatniego połączenia z Serwerem administracyjnym.

Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego zostało nawiązane ostatnie połączenie pomiędzy Agentem sieciowym zainstalowanym na urządzeniu klienckim a Serwerem administracyjnym. Wybór będzie zawierał urządzenia mieszczące się w określonym przedziale czasu.

Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

Domyślnie pole to nie jest zaznaczone.

- Nowe urządzenia odnalezione podczas skanowania sieci

Wyszukiwanie nowych urządzeń, które zostały wykryte podczas przeszukiwania sieci w przeciągu kilku ostatnich dni.

Jeśli ta opcja jest włączona, wybór będzie zawierał nowe urządzenia wykryte podczas wykrywania urządzeń w czasie określonym w polu **Okres wykrywania (dni)**.

Jeśli ta opcja jest wyłączona, wybór będzie zawierał wszystkie urządzenia wykryte podczas wykrywania urządzeń.

Domyślnie opcja ta jest wyłączona.

- Dostępność urządzenia

Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania:

- **Tak**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie widoczne w sieci.
- **Nie**. Aplikacja uwzględnia w wyborze urządzenia, które są aktualnie niewidoczne w sieci.
- **Nie wybrano wartości**. Kryterium nie będzie stosowane.

Aplikacja

W sekcji **Aplikacja** możesz skonfigurować kryteria uwzględniania urządzeń w wyborze w oparciu o wybraną zarządzaną aplikację:

- Nazwa aplikacji

  Na liście rozwijalnej możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji Kaspersky.

  Lista zawiera tylko nazwy aplikacji z wtyczkami administracyjnymi zainstalowanych na stacji roboczej administratora.

  Jeśli żadna aplikacja nie została wybrana, kryterium nie będzie stosowane.

- Wersja aplikacji

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według numeru wersji aplikacji Kaspersky.

  Jeśli żaden numer wersji nie został określony, kryterium nie będzie stosowane.

- Nazwa aktualizacji krytycznej

  W polu wejściowym możesz ustawić kryterium uwzględniania urządzeń w wyborze podczas wyszukiwania według nazwy aplikacji lub numeru pakietu aktualizacyjnego.

  Jeśli pole będzie puste, kryterium nie będzie stosowane.

- Ostatnia aktualizacja modułów

  Ta opcja może zostać użyta do ustawienia kryterium wyszukiwania urządzeń według godziny ostatniej aktualizacji modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole jest zaznaczone, w polach wejściowych możesz określić przedział czasu (datę i godzinę), w trakcie którego została wykonana ostatnia aktualizacja modułów aplikacji zainstalowanych na tych urządzeniach.

  Jeśli to pole nie jest zaznaczone, kryterium nie będzie stosowane.

  Domyślnie pole to nie jest zaznaczone.

- Urządzenie jest zarządzane przez Kaspersky Security Center 14

Korzystając z tej listy rozwijalnej, w wyborze możesz uwzględnić urządzenia zarządzane poprzez Kaspersky Security Center Linux:

- **Tak**. Aplikacja uwzględni w wyborze urządzenia zarządzane poprzez Kaspersky Security Center Linux.
- **Nie**. Aplikacja uwzględni w wyborze urządzenia, jeśli nie są one zarządzane przez Kaspersky Security Center Linux.
- **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 antywirusowego. W polach wejściowych możesz określić przedział czasu, w trakcie którego zostało wykonane ostatnie skanowanie antywirusowe.

  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

  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).

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, Wstrzymana, Uruchomiona, Niepowodzenie*).

- Stan ochrony serwerów współpracy

  Wyszukiwanie urządzeń według stanu ochrony serwerów współpracy (*Brak danych z urządzenia*, *Zatrzymana*, *Uruchamianie, Wstrzymana*, *Uruchomiona*, *Niepowodzenie*).

- Stan ochrony antywirusowej serwerów pocztowych

  Wyszukiwanie urządzeń według stanu ochrony dla serwerów pocztowych (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymana, Uruchomiona, Niepowodzenie*).

- Stan czujnika Endpoint Sensor

  Wyszukiwanie urządzeń według stanu komponentu Endpoint Sensor (*Brak danych z urządzenia, Zatrzymana, Uruchamianie, Wstrzymana, Uruchomiona, Niepowodzenie*).

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.

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. 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. Korzystając z OpenAPI, możesz stworzyć aplikację kliencką.

Możesz użyć pola wyszukiwania w prawej części ekranu, aby znaleźć potrzebne informacje w przewodniku po OpenAPI.

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 pomocniczego Serwera administracyjnego i usuwanie hierarchii Serwerów administracyjnych
Pobierz pliki listy sieci przez bramę połączenia	Możesz nawiązać połączenie z Agentem sieciowym na żądanym urządzeniu za pomocą	Dostosowanie punktów dystrybucji i bram

do określonego hosta	bramy połączenia, a następnie pobrać plik z listą sieci na swoje urządzenie.	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
Uruchom zadanie urządzenia	Możesz nawiązać połączenie z Agentem sieciowym na żądanym urządzeniu za pomocą bramy połączenia, a następnie pobrać żądane zadanie.	Ręczne uruchamianie zadania
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	Tworzenie zadania

	• 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.	
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.

Interakcja Kaspersky Security Center Web Console i innych rozwiązań Kaspersky

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.

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 14 Web Console i KATA/KEDR Web Console, możesz skonfigurować dostęp do KATA/KEDR Web Console bezpośrednio z poziomu interfejsu Kaspersky Security Center 14 Web Console.

W celu skonfigurowania dostępu do KATA / KEDR Web Console:

1. W oknie głównym aplikacji, w górnej części ekranu kliknij **Ustawienia konsoli**.
2. Z menu rozwijalnego wybierz **Integracja**.

   Zostanie otwarte okno Ustawienia konsoli.
3. Na zakładce **Integracja**, w polu **URL do KATA/KEDR Web Console** internetowy KATA/KEDR Web Console wprowadź adres internetowy 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 skonfigurować interakcję między Kaspersky Security Center a inną aplikacją lub rozwiązaniem Kaspersky, na przykład Kaspersky Managed Detection and Response (nazywane również MDR), musisz ustanowić połączenie w tle pomiędzy konsolą Kaspersky Security Center Web Console a Serwerem administracyjnym. Możesz nawiązać to połączenie tylko wtedy, jeśli Twoje konto ma uprawnienie Modyfikuj listy ACL obiektów w obszarze funkcyjnym **Cechy ogólne: Uprawnienia użytkownika.**

Możesz skonfigurować interakcję tylko między Kaspersky Managed Detection and Response a wersją Kaspersky Security Center dla systemu Windows.

Aby nawiązać połączenie w tle:

1. Z listy rozwijalnej **Ustawienia konsoli** wybierz **Integracja**.

   Zostanie otwarte okno **Ustawienia konsoli**.
2. Wybierz zakładkę **Integracja**.

3. W zakładce **Integracja** wybierz sekcję **Integracja**.

4. Ustaw przycisk przełącznika do nawiązywania połączenia w tle w pozycji: **Nawiąż połączenie w tle dla integracji WŁĄCZONO**.

5. 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 Kaspersky Security Center 14 Web Console i 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.

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 Linux lub w jednym z dodatkowych źródeł informacji o Kaspersky Security Cente Linuxr, skontaktuj się z działem pomocy technicznej. Specjaliści z działu pomocy technicznej odpowiedzą na wszystkie pytania związane z instalacją i użytkowaniem Kaspersky Security Center Linux.

Kaspersky zapewnia wsparcie dla Kaspersky Security Center Linux w trakcie jej cyklu życia (zobacz stronę zawierającą czas trwania wsparcia technicznego). 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 za pośrednictwem telefonu

Pomoc techniczna jest dostępna w języku polskim. Informacje dotyczące uzyskania wsparcia technicznego w Twoim regionie oraz dane kontaktowe pomocy technicznej można znaleźć na stronie internetowej działu pomocy technicznej Kaspersky Customer Service.

Przed skontaktowaniem się z działem pomocy technicznej przeczytaj zasady korzystania z pomocy technicznej.

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 Linux 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.

Znane problemy

Kaspersky Security Center Linux ma szereg ograniczeń, które nie są krytyczne dla działania aplikacji:

- W zadaniach Pobierz uaktualnienia do repozytorium *Serwera administracyjnego* i *Pobierz uaktualnienia do repozytoriów punktów dystrybucji* uwierzytelnianie użytkownika nie będzie działać, jeśli jako źródło uaktualnień wybierzesz chroniony hasłem folder lokalny lub sieciowy. Aby rozwiązać ten problem, najpierw zamontuj folder chroniony hasłem, a następnie określ wymagane poświadczenia, na przykład za pomocą systemu operacyjnego. Następnie możesz wybrać ten folder jako źródło aktualizacji w zadaniu pobierania aktualizacji. Kaspersky Security Center nie będzie wymagał wprowadzania danych uwierzytelniających.

- Zadanie *Zmień Serwer administracyjny* nie jest uruchamiane automatycznie po ustawieniu opcji **Natychmiast** w terminarzu zadań i zapisaniu zmian.

- Jeżeli określisz ustawienia serwera proxy we właściwościach serwera administracyjnego, a następnie włączysz opcję **Nie używaj serwera proxy** w zadaniu *Pobierz uaktualnienia do repozytorium serwera administracyjnego*, opcja ta zostanie zignorowana, a połączenie zostanie nawiązane za pośrednictwem serwera proxy.

- Jeżeli otworzysz Kaspersky Security Center 14 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.

- Ustawienia zablokowane w profilu nadrzędnym Kaspersky Endpoint Security for Linux są dziedziczone, ale nie są blokowane w profilach podrzędnych.

- Informacje o sprzęcie wysyłane z zarządzanego urządzenia do Serwera administracyjnego mogą nie być kompletne; niektóre elementy sprzętu mogą nie być określone.

- Kategorię aplikacji dodaną do funkcji Kontrola aplikacji w profilu Kaspersky Endpoint Security for Linux można usunąć.

- 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 określisz niestandardowe konta użytkownika w webConsoleAccount oraz parametry managementServiceAccount w pliku odpowiedzi na potrzeby instalacji Kaspersky Security Center 14 Web Console, a konta te należą do różnych grup bezpieczeństwa, Kaspersky Security Center 14 Web Console nie będzie działać po instalacji.

- W 64-bitowej wersji Astra Linux pakietu klnagent-astra nie można uaktualnić za pomocą pakietu klnagent64_14: stary pakiet klnagent64-astra zostanie usunięty, a nowy pakiet klnagent64 zostanie zainstalowany zamiast uaktualnienia, więc zostanie dodana nowa ikona urządzenia z pakietem klnagent64_14. Możesz usunąć starą ikonę tego urządzenia.

Słownik

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.

Aktywny klucz

Klucz, który jest aktualnie używany przez aplikację.

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.

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.

Certyfikatu Serwera administracyjnego

Certyfikat używany przez Serwer administracyjny do następujących celów:

- Uwierzytelnianie Serwera administracyjnego podczas łączenia się z Kaspersky Security Center 14 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.

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.

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.

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 (Private KSN)

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 użytkowników 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.

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.

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.

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.

Instalacja zdalna

Instalacja aplikacji firmy Kaspersky przy użyciu usług oferowanych przez Kaspersky Security Center Linux.

Grupa ról

Grupa użytkowników urządzeń mobilnych z Exchange ActiveSync, którzy uzyskali podobne uprawnienia administracyjne.

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.

Certyfikat współdzielony

Certyfikat, który jest przeznaczony do identyfikacji urządzenia mobilnego użytkownika.

Aktualizacja

Procedura zastępowania lub dodawania nowych plików (baz danych lub modułów aplikacji) pobieranych z serwerów aktualizacji firmy Kaspersky.

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.

Klient Serwera administracyjnego (urządzenie klienckie)

Urządzenie, serwer lub stacja robocza, na której zainstalowany jest Agent sieciowy i zarządzane aplikacje Kaspersky.

Konsola administracyjna

Składnik Kaspersky Security Center oparty na systemie Windows (zwany również Konsolą administracyjną opartą na MMC). Ten składnik zapewnia interfejs użytkownika dla usług administracyjnych Serwera administracyjnego i Agenta sieciowego. Konsola administracyjna jest odpowiednikiem Kaspersky Security Center 14 Web Console.

Kopia zapasowa danych Serwera administracyjnego

Kopiowanie przy użyciu narzędzia kopii zapasowej danych Serwera administracyjnego do miejsca przechowywania oraz ich późniejsze przywracanie. Narzędzie to umożliwia zapisanie:

- Bazy danych Serwera administracyjnego (zasady, zadania, ustawienia aplikacji, zdarzenia zapisane na Serwerze administracyjnym)
- Informacji o konfiguracji struktury grup administracyjnych i urządzeń klienckich
- Miejsc przechowywania plików instalacyjnych przeznaczonych do zdalnej instalacji aplikacji (zawartość folderów: Pakiety, Dezinstalacja uaktualnień)
- Certyfikatu Serwera administracyjnego

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 Linux.

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 konfiguracyjny

Zasada zawierająca zbiór ustawień i ograniczeń dla urządzenia mobilnego iOS MDM.

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 Linux.

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.

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.

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, z którego otwierasz Kaspersky Security Center 14 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.

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.

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.

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 w katalogu 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 zastrzeżonymi znakami towarowymi firmy Amazon.com, Inc. i/lub jej oddziałów, zarejestrowanymi w Stanach Zjednoczonych i/lub innych krajach.

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., zarejestrowanymi w Stanach Zjednoczonych i innych krajach i regionach.

Logo, marka i słowo Bluetooth należą do firmy Bluetooth SIG, Inc.

Ubuntu jest zastrzeżonym znakiem towarowym firmy Canonical Ltd.

Cisco, Cisco Systems, 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.

Dropbox jest zastrzeżonym znakiem towarowym firmy Dropbox, Inc.

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 i YouTube są zastrzeżonymi znakami towarowymi firmy Google, Inc.

FusionCompute, FusionSphere są znakami towarowymi firmy Huawei Technologies Co., Ltd, zarejestrowanymi w Chinach i innych krajach.

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.

Micro Focus to znak towarowy lub zastrzeżony znak towarowy firmy Micro Focus (IP) Limited lub jej oddziałów w Wielkiej Bytanii, Stanach Zjednoczonych i innych krajach.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista, oraz Windows Azure są znakami towarowymi grupy firm Microsoft.

Mozilla, Firefox, Thunderbird są znakami towarowymi firmy Mozilla Foundation.

Novell jest zastrzeżonym znakiem towarowym firmy Novell Enterprises Inc. w Stanach Zjednoczonych i innych krajach.

Oracle, Java, JavaScript i TouchDown są zastrzeżonymi znakami towarowymi firmy Oracle i/lub jej oddziałów.

Parallels i logo Parallels są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Parallels International GmbH w Kanadzie, Stanach Zjednoczonych i/lub w innych miejscach.

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, Ansible, CentOS, 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.

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.

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.