

kaspersky

Kaspersky Endpoint Security for Windows 11.7.0

© 2023 AO Kaspersky Lab

Spis treści

[Najczęściej zadawane pytania](#)

[Nowości](#)

[Kaspersky Endpoint Security for Windows](#)

[Pakiet dystrybucyjny](#)

[Wymagania sprzętowe i programowe](#)

[Porównanie dostępnych funkcji aplikacji w zależności od typu systemu operacyjnego](#)

[Porównanie funkcji aplikacji w zależności od narzędzi do zarządzania](#)

[Kompatybilność z innymi aplikacjami](#)

[Instalowanie i dezinstalowanie aplikacji](#)

[Wdrożenie za pośrednictwem Kaspersky Security Center](#)

[Standardowa instalacja aplikacji](#)

[Tworzenie pakietu instalacyjnego](#)

[Aktualizowanie baz danych w pakiecie instalacyjnym](#)

[Tworzenie zadania zdalnej instalacji](#)

[Instalowanie aplikacji lokalnie przy użyciu kreatora](#)

[Zdalne instalowanie aplikacji przy użyciu System Center Configuration Manager](#)

[Opis ustawień instalacji pliku setup.ini](#)

[Zmiana składników aplikacji](#)

[Aktualizowanie z poprzedniej wersji aplikacji](#)

[Dezinstalacja aplikacji](#)

[Dezinstalacja za pośrednictwem Kaspersky Security Center](#)

[Dezinstalowanie aplikacji przy użyciu Kreatora](#)

[Licencjonowanie aplikacji](#)

[Informacje o Umowie licencyjnej](#)

[Informacje o licencji](#)

[Informacje o certyfikacie licencji](#)

[Informacje o subskrypcji](#)

[Informacje o kluczu licencyjnym](#)

[Informacje o kodzie aktywacyjnym](#)

[Informacje o pliku klucza](#)

[Aktywowanie aplikacji](#)

[Aktywowanie aplikacji za pośrednictwem Kaspersky Security Center](#)

[Aktywacja aplikacji za pomocą Kreatora aktywacji](#)

[Przeglądanie informacji o licencji](#)

[Kupowanie licencji](#)

[Odnawianie subskrypcji](#)

[Przekazywanie danych](#)

[Przekazywanie danych zgodnie z Umową licencyjną](#)

[Przekazywanie danych podczas korzystania z Kaspersky Security Network](#)

[Przekazywanie danych podczas korzystania z rozwiązań Detection and Response](#)

[Aktywowanie Kaspersky Endpoint Detection and Response](#)

[Kaspersky Sandbox](#)

[Zgodność z prawem Unii Europejskiej.\(RODO\)](#)

[Rozpoczęcie pracy](#)

[Informacje o wtyczce zarządzającej Kaspersky Endpoint Security for Windows](#)

[Kwestie specjalne dotyczące pracy z różnymi wersjami wtyczek zarządzających](#)

[Kwestie specjalne podczas używania zaszyfrowanych protokołów do interakcji z zewnętrznymi usługami](#)

[Interfejs aplikacji](#)

[Ikona aplikacji w obszarze powiadomień paska zadań](#)

[Uproszczony interfejs aplikacji](#)

[Konfigurowanie wyświetlania interfejsu aplikacji](#)

[Rozpoczęcie pracy](#)

[Zarządzanie profilami](#)

[Zarządzanie zadaniami](#)

[Konfigurowanie lokalnych ustawień aplikacji](#)

[Uruchamianie i zatrzymywanie Kaspersky Endpoint Security](#)

[Wstrzymywanie i wznowianie kontroli i ochrony komputera](#)

[Skanowanie antywirusowe komputera](#)

[Skanowanie komputera](#)

[Skanowanie napędów wymiennych po ich podłączeniu do komputera](#)

[Skanowanie w tle](#)

[Skanowanie z menu kontekstowego](#)

[Sprawdzanie integralności aplikacji](#)

[Modyfikowanie obszaru skanowania](#)

[Uruchamianie zaplanowanego skanowania](#)

[Uruchamianie skanowania jako inny użytkownik](#)

[Optymalizacja skanowania](#)

[Aktualizowanie baz danych i modułów aplikacji](#)

[Scenariusze aktualizacji baz danych i modułów aplikacji](#)

[Aktualizowanie z repozytorium serwera](#)

[Aktualizowanie z folderu współdzielonego](#)

[Aktualizowanie przy użyciu narzędzia Kaspersky Update Utility](#)

[Aktualizowanie w trybie mobilnym](#)

[Uruchamianie i zatrzymywanie zadania aktualizacji](#)

[Uruchamianie zadania aktualizacji z poziomu konta innego użytkownika](#)

[Wybieranie trybu uruchamiania zadania aktualizacji](#)

[Dodawanie źródła uaktualnień](#)

[Konfigurowanie aktualizacji z foldera współdzielonego](#)

[Aktualizowanie modułów aplikacji](#)

[Używanie serwera proxy do aktualizacji](#)

[Wycofanie ostatniej aktualizacji](#)

[Praca z aktywnymi zagrożeniami](#)

[Ochrona komputera](#)

[Ochrona plików](#)

[Włączanie i wyłączanie modułu Ochrona plików](#)

[Automatyczne wstrzymywanie Ochrony plików](#)

[Zmienianie akcji wykonywanej na zainfekowanych plikach przez moduł Ochrona plików](#)

[Tworzenie obszaru ochrony modułu Ochrona plików](#)

[Używanie metod skanowania](#)

[Używanie technologii skanowania w działaniu modułu Ochrona plików](#)

[Optymalizowanie skanowania plików](#)

[Skanowanie plików złożonych](#)

[Zmienianie trybu skanowania](#)

[Ochrona WWW](#)

[Włączanie i wyłączanie modułu Ochrona WWW](#)

[Zmianianie akcji podejmowanej na szkodliwych obiektach w ruchu sieciowym](#)

[Skanowanie adresów internetowych z wykorzystaniem baz danych phishingowych i szkodliwych adresów internetowych](#)

[Używanie analizy heurystycznej w działaniu modułu Ochrona WWW](#)

[Tworzenie listy zaufanych adresów internetowych](#)

[Eksportowanie i importowanie listy zaufanych adresów internetowych](#)

[Ochrona poczty](#)

[Włączanie i wyłączanie modułu Ochrona poczty](#)

[Zmianianie akcji podejmowanej na zainfekowanych wiadomościach e-mail](#)

[Tworzenie obszaru ochrony modułu Ochrona poczty](#)

[Skanowanie plików złożonych załączonych do wiadomości e-mail](#)

[Filtrowanie załączników wiadomości e-mail](#)

[Eksportowanie i importowanie rozszerzeń dla filtrowania załączników](#)

[Skanowanie poczty elektronicznej w programie Microsoft Office Outlook](#)

[Ochrona sieci](#)

[Włączanie i wyłączanie modułu Ochrona sieci](#)

[Blokowanie atakującego komputera](#)

[Konfigurowanie wykluczania adresów z blokowania](#)

[Eksportowanie i importowanie listy wykluczeń z blokowania](#)

[Konfigurowanie ochrony przed atakami sieciowymi według typu](#)

[Zapora sieciowa](#)

[Włączanie i wyłączanie modułu Zapora sieciowa](#)

[Zmianianie stanu połączenia sieciowego](#)

[Zarządzanie regułami dla pakietów sieciowych](#)

[Tworzenie reguły dla pakietu sieciowego](#)

[Włączanie i wyłączanie reguły dla pakietu sieciowego](#)

[Zmianianie akcji Zapory sieciowej dla reguły dla pakietu sieciowego](#)

[Zmianianie priorytetu reguły dla pakietu sieciowego](#)

[Eksportowanie i importowanie reguł dla pakietów sieciowych](#)

[Zarządzanie regułami sieciowymi dla aplikacji](#)

[Tworzenie reguły sieciowej dla aplikacji](#)

[Włączanie i wyłączanie reguły sieciowej dla aplikacji](#)

[Zmianianie akcji Zapory sieciowej dla reguły sieciowej dla aplikacji](#)

[Zmianianie priorytetu reguły sieciowej dla aplikacji](#)

[Monitor sieci](#)

[Ochrona przed atakami BadUSB](#)

[Włączanie i wyłączanie Ochrony przed atakami BadUSB](#)

[Korzystanie z Klawiatury ekranowej do autoryzacji urządzeń USB](#)

[Ochrona AMSI](#)

[Włączanie i wyłączanie Ochrony AMSI](#)

[Używanie Ochrony AMSI do skanowania plików złożonych](#)

[Ochrona przed exploitami](#)

[Włączanie i wyłączanie modułu Ochrona przed exploitami](#)

[Wybieranie działania, jakie ma zostać wykonane po wykryciu exploita](#)

[Ochrona pamięci procesów systemowych](#)

[Wykrywanie zachowań](#)

[Włączanie i wyłączanie modułu Wykrywanie zachowań](#)

[Wybieranie działania, jakie ma zostać podjęte po wykryciu szkodliwej aktywności](#)

[Ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym](#)

[Włączanie i wyłączanie ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym](#)

[Wybieranie działania, jakie ma zostać wykonane po wykryciu szyfrowania zewnętrznego folderów współdzielonych](#)

[W celu włączenia ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym:](#)

[Konfigurowanie adresów komputerów dla wykluczeń z ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym](#)

[Eksportowanie i importowanie listy wykluczeń z ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem](#)

[Ochrona przed włamaniami](#)

[Włączanie i wyłączanie modułu Ochrona przed włamaniami](#)

[Zarządzanie grupami zaufania aplikacji](#)

[Zmiana grupy zaufania aplikacji](#)

[Konfigurowanie uprawnień grupy zaufania](#)

[Wybieranie grupy zaufania dla aplikacji uruchamianych przed Kaspersky Endpoint Security](#)

[Wybieranie grupy zaufania dla nieznanych aplikacji](#)

[Wybieranie grupy zaufania dla cyfrowo podpisanych aplikacji](#)

[Zarządzanie uprawnieniami aplikacji](#)

[Ochrona zasobów systemu operacyjnego i danych osobowych](#)

[Usuwanie informacji o nieużywanych aplikacjach](#)

[Monitorowanie Ochrony przed włamaniami](#)

[Ochrona dostępu do audio i wideo](#)

[Silnik korygujący](#)

[Kaspersky Security Network](#)

[Włączanie i wyłączanie korzystania z Kaspersky Security Network](#)

[Ograniczenia Private KSN](#)

[Włączanie i wyłączanie dla składników ochrony trybu chmury](#)

[Sprawdzanie reputacji pliku w Kaspersky Security Network](#)

[Skanowanie połączeń szyfrowanych](#)

[Konfigurowanie ustawień skanowania połączeń szyfrowanych](#)

[Skanowanie połączeń szyfrowanych w Firefox i Thunderbird](#)

[Wyłączanie połączeń szyfrowanych ze skanowania](#)

[Kontrola komputera](#)

[Kontrola sieci](#)

[Włączanie i wyłączanie modułu Kontrola sieci](#)

[Działania podejmowane na regułach dostępu do zasobów sieciowych](#)

[Dodawanie reguły dostępu do zasobu sieciowego](#)

[Przydzielanie priorytetów do reguł dostępu do zasobów sieciowych](#)

[Włączanie i wyłączanie reguły dostępu do zasobu sieciowego](#)

[Eksportowanie i importowanie listy zaufanych adresów internetowych](#)

[Testowanie reguł dostępu do zasobów sieciowych](#)

[Eksportowanie i importowanie listy adresów zasobów sieciowych](#)

[Monitorowanie aktywności użytkownika w internecie](#)

[Modyfikowanie szablonów wiadomości Kontroli sieci](#)

[Modyfikowanie masek adresów zasobów sieciowych](#)

[Przenoszenie reguł dostępu do zasobów sieciowych z poprzedniej wersji aplikacji](#)

[Kontrola urządzeń](#)

[Włączanie i wyłączanie modułu Kontrola urządzeń](#)

[Informacje o regułach dostępu](#)

[Modyfikowanie reguły dostępu do urządzenia](#)

- [Modyfikowanie reguły dostępu do magistrali połączeń](#)
- [Dodawanie sieci Wi-Fi do listy zaufanych](#)
- [Monitorowanie korzystania z nośników wymiennych](#)
- [Zmiana czasu trwania buforowania](#)
- [Działania podejmowane na zaufanych urządzeniach](#)
 - [Dodawanie urządzenia do listy Zaufane z poziomu interfejsu aplikacji](#)
 - [Dodawanie urządzenia do listy Zaufane z poziomu Kaspersky Security Center](#)
 - [Eksportowanie i importowanie listy zaufanych urządzeń](#)
- [Uzyskiwanie dostępu do zablokowanego urządzenia](#)
 - [Tryb online dla zezwalania na dostęp](#)
 - [Tryb offline dla zezwalania na dostęp](#)
- [Modyfikowanie szablonów wiadomości Kontroli urządzeń](#)
- [Anti-Bridging](#)
 - [Włączanie modułu Anti-Bridging](#)
 - [Zmiana stanu reguły połączenia](#)
 - [Zmiana priorytetu reguły połączenia](#)
- [Adaptacyjna kontrola anomalii](#)
 - [Włączanie i wyłączanie Adaptacyjnej kontroli anomalii](#)
 - [Włączanie i wyłączanie reguły Adaptacyjnej kontroli anomalii](#)
 - [Modyfikowanie akcji podejmowanej w momencie wyzwolenia reguły Adaptacyjnej kontroli anomalii](#)
 - [Tworzenie wykluczeń dla reguły Adaptacyjnej kontroli anomalii](#)
 - [Eksportowanie i importowanie wykluczeń dla reguł Adaptacyjnej kontroli anomalii](#)
 - [Stosowanie aktualizacji dla reguł Adaptacyjnej kontroli anomalii](#)
 - [Modyfikowanie szablonów wiadomości Adaptacyjnej kontroli anomalii](#)
 - [Przeglądanie raportów Adaptacyjnej kontroli anomalii](#)
- [Kontrola aplikacji](#)
 - [Ograniczenia funkcjonalności Kontroli aplikacji](#)
 - [Włączanie i wyłączanie modułu Kontrola aplikacji](#)
 - [Wybieranie trybu Kontroli aplikacji](#)
 - [Praca z regułami Kontroli aplikacji w interfejsie aplikacji](#)
 - [Dodawanie reguły Kontroli aplikacji](#)
 - [Dodawanie warunku wyzwającego dla reguły Kontroli aplikacji](#)
 - [Zmianie stanu reguły Kontroli aplikacji](#)
- [Zarządzanie regułami Kontroli aplikacji w Kaspersky Security Center](#)
 - [Otrzymywanie informacji o aplikacjach zainstalowanych na komputerach użytkowników](#)
 - [Tworzenie kategorii aplikacji](#)
 - [Dodawanie plików wykonywalnych z folderu Pliki wykonywalne do kategorii aplikacji](#)
 - [Dodawanie plików wykonywalnych związanych ze zdarzeniami do kategorii aplikacji](#)
 - [Dodawanie i modyfikowanie reguły Kontroli aplikacji przy użyciu Kaspersky Security Center](#)
 - [Zmianie stanu reguły Kontroli aplikacji przy użyciu Kaspersky Security Center](#)
 - [Eksportowanie i importowanie reguł Kontroli aplikacji](#)
 - [Testowanie reguł Kontroli aplikacji przy użyciu Kaspersky Security Center](#)
 - [Przeglądanie zdarzeń z działania testowego komponentu Kontrola aplikacji](#)
 - [Przeglądanie raportu dotyczącego zablokowanych aplikacji w trybie testowym](#)
 - [Przeglądanie zdarzeń z działania modułu Kontrola aplikacji](#)
 - [Przeglądanie raportu dotyczącego zablokowanych aplikacji](#)
- [Testowanie działania reguł Kontroli aplikacji](#)
- [Monitor aktywności aplikacji](#)

- [Reguły tworzenia masek nazw dla plików i folderów](#)
- [Modyfikowanie szablonów wiadomości Kontroli aplikacji](#)
- [Praktyczne zastosowanie aplikacji w celu zaimplementowania listy dozwolonych aplikacji](#)
 - [Konfigurowanie trybu listy zezwolonych aplikacji](#)
 - [Testowanie trybu listy zezwolonych](#)
 - [Obsługa listy zezwolonych aplikacji](#)
- [Monitorowanie portów sieciowych](#)
 - [Włączanie monitorowania wszystkich portów sieciowych](#)
 - [Tworzenie listy monitorowanych portów sieciowych](#)
 - [Tworzenie listy aplikacji, dla których monitorowane są wszystkie porty sieciowe](#)
 - [Eksportowanie i importowanie list monitorowanych portów](#)
- [Wyczyść dane](#)
- [Ochrona hasłem](#)
 - [Włączanie ochrony hasłem](#)
 - [Nadawanie uprawnień pojedynczym użytkownikom lub grupom](#)
 - [Używanie hasła tymczasowego do nadawania uprawnień](#)
 - [Specjalne kwestie dotyczące uprawnień Ochrony hasłem](#)
- [Strefa zaufana](#)
 - [Tworzenie wykluczenia ze skanowania](#)
 - [Włączanie i wyłączanie wykluczenia ze skanowania](#)
 - [Modyfikowanie listy zaufanych aplikacji](#)
 - [Włączanie i wyłączanie reguł strefy zaufanej dla aplikacji na liście zaufanych aplikacji](#)
 - [Korzystanie z magazynu zaufanych certyfikatów systemowych](#)
- [Zarządzanie Kopią zapasową](#)
 - [Konfigurowanie maksymalnego okresu przechowywania plików w Kopii zapasowej](#)
 - [Konfigurowanie maksymalnego rozmiaru Kopii zapasowej](#)
 - [Przywracanie plików z Kopii zapasowej](#)
 - [Usuwanie kopii zapasowych plików z Kopii zapasowej](#)
- [Usługa powiadomień](#)
 - [Konfigurowanie ustawień dziennika zdarzeń](#)
 - [Konfigurowanie wyświetlania i dostarczania powiadomień](#)
 - [Konfigurowanie wyświetlania komunikatów o stanie aplikacji w obszarze powiadomień](#)
- [Zarządzanie raportami](#)
 - [Wyświetlanie raportów](#)
 - [Konfigurowanie maksymalnego czasu przechowywania raportu](#)
 - [Konfigurowanie maksymalnego rozmiaru pliku raportu](#)
 - [Zapisywanie raportu do pliku](#)
 - [Czyszczenie raportów](#)
- [Autoochrona Kaspersky Endpoint Security](#)
 - [Włączanie i wyłączanie Autoochrony](#)
 - [Włączanie i wyłączanie obsługi AM-PPL](#)
 - [Włączanie i wyłączanie ochrony przed zewnętrznym zarządzaniem](#)
 - [Obsługiwanie aplikacji do zdalnej administracji](#)
- [Działanie Kaspersky Endpoint Security i kompatybilność z innymi aplikacjami](#)
 - [Wybieranie typów wykrywanych obiektów](#)
 - [Włączanie i wyłączanie technologii zaawansowanego leczenia](#)
 - [Włączanie i wyłączanie trybu oszczędzania energii](#)
 - [Włączanie i wyłączanie udostępniania zasobów innym aplikacjom](#)

[Tworzenie i korzystanie z pliku konfiguracyjnego](#)

[Przywracanie ustawień domyślnych aplikacji](#)

[Przesyłanie wiadomości między użytkownikami a administratorem](#)

[Szyfrowanie danych](#)

[Ograniczenia funkcji szyfrowania](#)

[Zmiana długości klucza szyfrowania \(AES56 / AES256\)](#)

[Kaspersky Disk Encryption](#)

[Specjalne funkcje szyfrowania dysku SSD](#)

[Szyfrowanie całego dysku przy użyciu technologii Kaspersky Disk Encryption](#)

[Tworzenie listy dysków twardek wykluczonych z szyfrowania](#)

[Eksportowanie i importowanie listy dysków twardek wykluczonych z szyfrowania](#)

[Włączanie technologii Single Sign-On \(SSO\)](#)

[Zarządzanie kontami Agenta autoryzacji](#)

[Używanie tokenów i kart inteligentnych z Agentem autoryzacji](#)

[Deszyfrowanie dysków twardek](#)

[Przywracanie dostępu do dysku chronionego przez technologię Kaspersky Disk Encryption](#)

[Aktualizowanie systemu operacyjnego](#)

[Eliminowanie błędów aktualizacji funkcjonalności szyfrowania](#)

[Wybieranie poziomu śledzenia Agenta autoryzacji](#)

[Modyfikowanie komunikatów pomocy Agenta Autoryzacji](#)

[Usuwanie obiektów i danych pozostałych po testowym działaniu Agenta autoryzacji](#)

[Zarządzanie BitLocker](#)

[Uruchamianie Szyfrowania dysków funkcją BitLocker](#)

[Deszyfrowanie dysku twardego chronionego przez funkcję BitLocker](#)

[Przywracanie dostępu do dysku chronionego funkcją BitLocker](#)

[Wstrzymywanie ochrony funkcją BitLocker w celu zaktualizowania oprogramowania](#)

[Szyfrowanie na poziomie plików na lokalnych dyskach komputera](#)

[Szyfrowanie plików na lokalnych dyskach komputera](#)

[Tworzenie reguł dostępu do zaszyfrowanego pliku dla aplikacji](#)

[Szyfrowanie plików utworzonych lub zmodyfikowanych przez określone aplikacje](#)

[Generowanie reguły deszyfrowania](#)

[Deszyfrowanie plików na lokalnych dyskach komputera](#)

[Tworzenie zaszyfrowanych pakietów](#)

[Przywracanie dostępu do zaszyfrowanych plików](#)

[Przywracanie dostępu do zaszyfrowanych danych po awarii systemu operacyjnego](#)

[Modyfikowanie szablonów wiadomości dostępu do zaszyfrowanego pliku](#)

[Szyfrowanie nośników wymiennych](#)

[Uruchamianie szyfrowania nośników wymiennych](#)

[Dodawanie reguły szyfrowania dla nośników wymiennych](#)

[Eksportowanie i importowanie listy reguł szyfrowania dla nośników wymiennych](#)

[Tryb przenośny dla uzyskiwania dostępu do zaszyfrowanych plików na dyskach wymiennych](#)

[Deszyfrowanie nośników wymiennych](#)

[Przeglądanie informacji szczegółowych dotyczących szyfrowania danych](#)

[Sprawdzanie stanu szyfrowania](#)

[Przeglądanie statystyk szyfrowania dotyczących pulpitu nawigacyjnego Kaspersky Security Center](#)

[Przeglądanie błędów szyfrowania plików na lokalnych dyskach komputera](#)

[Przeglądanie raportu z szyfrowania danych](#)

[Praca z zaszyfrowanymi urządzeniami, gdy nie ma dostępu do nich](#)

[Odzyskiwanie danych za pomocą narzędzia przywracania FDERT](#)

[Tworzenie dysku ratunkowego systemu operacyjnego](#)

Detection and Response

[Kaspersky Endpoint Agent](#)

[Migrowanie konfiguracji \[KES+KEA\] do \[KES11.70\]](#)

[Managed Detection and Response](#)

[Endpoint Detection and Response](#)

[Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa \(IOC\)](#)

[Przenieś plik do Kwarantanny](#)

[Uzyskaj plik](#)

[Usuń plik](#)

[Rozpoczęcie procesu](#)

[Kończenie działania procesu](#)

[Zapobieganie wykonywaniu](#)

[Izolacja sieci komputerowej](#)

[Kaspersky Sandbox](#)

Zarządzanie aplikacją z poziomu wiersza poleceń

[Instalowanie aplikacji](#)

[Aktywowanie aplikacji](#)

[Deinstalacja aplikacji](#)

[Polecenia AVP](#)

[SCAN. Skanowanie antywirusowe](#)

[UPDATE. Aktualizowanie baz danych i modułów aplikacji](#)

[ROLLBACK. Wycofanie ostatniej aktualizacji](#)

[TRACES. Śledzenie](#)

[START. Uruchamianie profilu](#)

[STOP. Zatrzymywanie profilu](#)

[STATUS. Stan profilu](#)

[STATISTICS. Statystyki działania profilu](#)

[RESTORE. Przywracanie plików z Kopii zapasowej](#)

[EXPORT. Eksportowanie ustawień aplikacji](#)

[IMPORT. Importowanie ustawień aplikacji](#)

[ADDKEY. Zastosowanie pliku klucza](#)

[LICENSE. Licencjonowanie](#)

[RENEW. Kupowanie licencji](#)

[PBATESTRESET. Resetowanie wyników sprawdzania dysku przed zaszyfrowaniem dysku](#)

[EXIT. Zakończenie działania aplikacji](#)

[EXITPOLICY. Wyłączenie profilu](#)

[STARTPOLICY. Włączenie profilu](#)

[DISABLE. Wyłączenie ochrony](#)

[SPYWARE. Wykrywanie oprogramowania szpiegującego](#)

[KSN. Przeniesienie Globalnej / Prywatnej sieci KSN](#)

[Polecenia KESCLI](#)

[Skanowanie. Skanowanie antywirusowe](#)

[GetScanState. Stan zakończenia skanowania](#)

[GetLastScanTime. Określanie czasu zakończenia skanowania](#)

[GetThreats. Uzyskiwanie danych dotyczących wykrytych zagrożeń](#)

[UpdateDefinitions. Aktualizowanie baz danych i modułów aplikacji](#)

[GetDefinitionState. Określanie czasu zakończenia aktualizacji](#)

[EnableRTP. Włączanie ochrony](#)

[GetRealTimeProtectionState. Stan Ochrony plików](#)

[Wersja. Identyfikowanie wersji aplikacji](#)

[Polecenia zarządzania Detection and Response](#)

[SANDBOX. Zarządzanie Kaspersky Sandbox](#)

[PREVENTION. Zarządzanie zapobieganiem wykonaniu](#)

[ISOLATION. Zarządzanie Izolacją sieci](#)

[RESTORE. Przywracanie plików z Kwarantanny](#)

[start locScanTask. Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa \(IOC\)](#)

[MDRLICENSE. Aktywacja MDR](#)

[Kody błędów](#)

[Dodatek. Profile aplikacji](#)

[Zarządzanie aplikacją za pośrednictwem interfejsu API REST](#)

[Instalowanie aplikacji za pośrednictwem interfejsu API REST](#)

[Praca z interfejsem API](#)

[Źródła informacji o aplikacji](#)

[Kontakt z działem pomocy technicznej](#)

[Zawartość i przechowywanie plików śledzenia](#)

[Śledzenie działania aplikacji](#)

[Śledzenie wydajności aplikacji](#)

[Zapisywanie zrzutu pamięci](#)

[Ochrona plików zrzutu i plików śledzenia](#)

[Ograniczenia i uwagi](#)

[Słownik](#)

[Agent autoryzacji](#)

[Agent sieciowy](#)

[Aktywny klucz](#)

[Antywirusowe bazy danych](#)

[Archiwum](#)

[Baza adresów phishingowych](#)

[Baza danych szkodliwych adresów internetowych](#)

[Certyfikat licencji](#)

[Fałszywy alarm](#)

[Grupa administracyjna](#)

[IOC](#)

[Klucz dodatkowy](#)

[Leczenie](#)

[Maska](#)

[Obiekt OLE](#)

[Obszar ochrony](#)

[Obszar skanowania](#)

[OpenIOC](#)

[Plik infekowalny](#)

[Plik IOC](#)

[Przenośny menedżer plików](#)

[Trusted Platform Module \(moduł TPM\)](#)

[Wystawca certyfikatu](#)

[Zadanie](#)

[Zainfekowany plik](#)

[Znormalizowana postać adresu zasobu sieciowego](#)

[Dodatki](#)

[Dodatek 1. Ustawienia aplikacji](#)

[Ochrona plików](#)

[Ochrona WWW](#)

[Ochrona poczty](#)

[Ochrona sieci](#)

[Zapora sieciowa](#)

[Ochrona przed atakami BadUSB](#)

[Ochrona AMSI](#)

[Ochrona przed exploitami](#)

[Wykrywanie zachowań](#)

[Ochrona przed włamaniami](#)

[Silnik korygujący](#)

[Kaspersky Security Network](#)

[Kontrola sieci](#)

[Kontrola urządzeń](#)

[Kontrola aplikacji](#)

[Adaptacyjna kontrola anomalii](#)

[Endpoint Sensor](#)

[Kaspersky Sandbox](#)

[Endpoint Detection and Response](#)

[Szyfrowanie całego dysku](#)

[Szyfrowanie plików](#)

[Szyfrowanie nośników wymiennych](#)

[Szablony \(szyfrowanie danych\)](#)

[Wykluczenia](#)

[Ustawienia aplikacji](#)

[Raporty i pliki danych](#)

[Ustawienia sieci](#)

[Interfejs](#)

[Zarządzaj ustawieniami](#)

[Aktualizowanie baz danych i modułów aplikacji](#)

[Dodatek 2. Grupy zaufania aplikacji](#)

[Dodatek 3. Rozszerzenia plików do szybkiego skanowania dysków wymiennych](#)

[Dodatek 4. Typy plików dla filtra załączników modułu Ochrona poczty](#)

[Dodatek 5. Ustawienia sieci do interakcji z usługami zewnętrznymi](#)

[Dodatek 6. Zdarzenia aplikacji w dzienniku zdarzeń systemu Windows](#)

[Dodatek 7. Zdarzenia aplikacji w dzienniku zdarzeń Kaspersky Security Center](#)

[Dodatek 8. Obsługiwane rozszerzenia plików dla Zapobiegania wykonywaniu](#)

[Dodatek 9. Obsługiwane interpretatory skryptów](#)

[Dodatek 10. Obszar skanowania IOC w rejestrze \(RegistryItem\)](#)

[Dodatek 11. Wymagania pliku IOC](#)

[Informacje o kodzie firm trzecich](#)

[Informacje o znakach towarowych](#)

Najczęściej zadawane pytania



OGÓLNE

[Na jakich komputerach może działać Kaspersky Endpoint Security?](#)

[Co się zmieniło od ostatniej wersji?](#)

[Z jakimi innymi aplikacjami Kaspersky może działać Kaspersky Endpoint Security?](#)

[Jak można oszczędzić zasoby komputera podczas działania Kaspersky Endpoint Security?](#)



WDRAŻANIE

[Jak zainstalować Kaspersky Endpoint Security na wszystkich komputerach w organizacji?](#)

[Które ustawienia instalacji mogą zostać skonfigurowane z poziomu wiersza poleceń?](#)

[Jak zdalnie odinstalować Kaspersky Endpoint Security?](#)



AKTUALIZACJA

[Jakie metody są dostępne do aktualizowania baz danych?](#)

[Co należy zrobić, jeśli po aktualizacji wystąpią problemy?](#)

[W jaki sposób można zaktualizować bazy danych poza siecią korporacyjną?](#)

[Czy możliwe jest używanie serwera proxy dla aktualizacji?](#)



BEZPIECZEŃSTWO

[W jaki sposób Kaspersky Endpoint Security skanuje wiadomości e-mail?](#)

[Jak można wykluczyć zaufany plik ze skanowania?](#)

[Jak można chronić komputer przed wirusami z dysków flash?](#)

[Jak uruchamiać skanowanie antywirusowe ukryte przed użytkownikiem?](#)

[W jaki sposób tymczasowo wstrzymać ochronę Kaspersky Endpoint Security?](#)

[Jak przywrócić plik, który został pomyłkowo usunięty przez Kaspersky Endpoint Security?](#)



INTERNET

[Czy Kaspersky Endpoint Security skanuje połączenia szyfrowane \(HTTPS\)?](#)

[Jak zezwolić użytkownikom na nawiązywanie połączenia tylko z zaufanymi sieciami Wi-Fi?](#)

[Jak zablokować sieci społecznościowe?](#)



APLIKACJE

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

[Jak uniemożliwić uruchamianie gier komputerowych?](#)

[Jak mogę sprawdzić, czy Kontrola aplikacji została poprawnie skonfigurowana?](#)

[Jak dodać aplikację do listy zaufanych?](#)



URZĄDZENIA

[Jak można zablokować korzystanie z dysków flash?](#)

[Jak dodać urządzenie do listy zaufanych?](#)

[Czy możliwe jest uzyskanie dostępu do zablokowanego urządzenia?](#)



SZYFROWANIE

[W jakich warunkach szyfrowanie jest niemożliwe?](#)

[Jak można używać hasła do ograniczenia dostępu do archiwum?](#)

[Czy możliwe jest używanie kart inteligentnych i tokenów z szyfrowaniem?](#)

[Czy możliwe jest uzyskanie dostępu do zaszyfrowanych danych, jeśli nie ma połączenia z Kaspersky Security Center?](#)

[Co należy zrobić, jeśli wystąpi błąd systemu operacyjnego komputera, a dane pozostaną zaszyfrowane?](#)



POMOC TECHNICZNA

[Gdzie jest przechowywany plik raportu?](#)

[Jak można utworzyć plik śledzenia?](#)

[Jak można włączyć zapisywanie zrzutu pamięci?](#)

Nowości

Aktualizacja 11.7.0

Program Kaspersky Endpoint Security for Windows 11.7.0 oferuje następujące nowe funkcje i ulepszenia:

1. Zaktualizowano [interfejs Kaspersky Endpoint Security for Windows](#).
2. [Obsługa systemu Windows 11, Windows 10 21H2 i Windows Server 2022](#).
3. Dodano nowe składniki:
 - Dodano [wbudowanego agenta do integracji z Kaspersky Sandbox](#). *Rozwiązanie Kaspersky Sandbox wykrywa i automatycznie blokuje zaawansowane zagrożenia na komputerach. Kaspersky Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Kaspersky Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Kaspersky Sandbox). Więcej informacji o rozwiązaniu można znaleźć w [pomocy dla Kaspersky Sandbox](#).*

Aby korzystać z Kaspersky Sandbox, niepotrzebny jest już Kaspersky Endpoint Agent. Kaspersky Endpoint Security może wykonywać wszystkie funkcje Kaspersky Endpoint Agent. Aby migrować zasady Kaspersky Endpoint Agent, użyj [Kreatora migracji](#). Potrzebujesz Kaspersky Security Center 13.2 do działania wszystkich funkcji Kaspersky Sandbox. Więcej informacji o migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows znajdziesz w [pomocy aplikacji](#).
 - [Dodano wbudowanego agenta do obsługi działania rozwiązania Kaspersky Endpoint Detection and Response Optimum](#). *Kaspersky Endpoint Detection and Response Optimum to rozwiązanie do ochrony infrastruktury IT organizacji przed zaawansowanymi cyberzagrożeniami. Funkcjonalność rozwiązania łączy automatyczne wykrywanie zagrożeń z możliwością reagowania na te zagrożenia w celu przeciwdziałania zaawansowanym atakom, w tym nowym exploitom, oprogramowaniu ransomware, atakom bezplikowym, a także metodom z użyciem legalnych narzędzi systemowych. Więcej informacji o rozwiązaniu znajdziesz w [pomocy dla Kaspersky Endpoint Detection and Response Optimum](#).*

Aby korzystać z Kaspersky Endpoint Detection and Response, niepotrzebny jest już Kaspersky Endpoint Agent. Kaspersky Endpoint Security może wykonywać wszystkie funkcje Kaspersky Endpoint Agent. Aby migrować zasady i zadania Kaspersky Endpoint Agent, użyj [Kreatora migracji](#). Do korzystania ze wszystkich funkcji Kaspersky Endpoint Detection and Response Optimum wymaga Kaspersky Security Center 13.2. Więcej informacji o migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows znajdziesz w [pomocy aplikacji](#).
4. Dodano [Kreator migracji](#) dla zasad i zadań Kaspersky Endpoint Agent. Kreator migracji tworzy nowe scalone zasady i zadania dla Kaspersky Endpoint Security for Windows. Kreator umożliwia przełączenie rozwiązań Detection and Response z Kaspersky Endpoint Agent do Kaspersky Endpoint Security. Rozwiązania Detection and Response zawierają Kaspersky Sandbox, Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) oraz Kaspersky Managed Detection and Response (MDR).
5. [Kaspersky Endpoint Agent](#), który jest zawarty w pakiecie dystrybucyjnym, został zaktualizowany do wersji 3.11.

Podczas aktualizacji Kaspersky Endpoint Security aplikacja wykrywa wersję i wyznaczony cel Kaspersky Endpoint Agent. Jeśli Kaspersky Endpoint Agent jest przeznaczony do działania Kaspersky Sandbox, Kaspersky Managed Detection and Response (MDR) oraz Kaspersky Endpoint Detection and Response Optimum (EDR Optimum), Kaspersky Endpoint Security przełączy działanie tych rozwiązań do wbudowanego agenta aplikacji. W przypadku Kaspersky Sandbox and EDR Optimum aplikacja automatycznie odinstalowuje Kaspersky Endpoint Agent. Jeśli chodzi o MDR, możesz ręcznie odinstalować Kaspersky Endpoint Agent. Jeśli aplikacja jest przeznaczona do użycia w celu zapewnienia działania Kaspersky Endpoint Detection and Response Expert (EDR Expert), Kaspersky Endpoint Security zaktualizuje wersję Kaspersky Endpoint Agent. Więcej informacji o aplikacji można znaleźć w dokumentacji do rozwiązań firmy Kaspersky, które obsługują Kaspersky Endpoint Agent.

6. Udoskonalono funkcjonalność Szyfrowanie funkcją BitLocker:

- Rozszerzony kod PIN może być teraz używany z funkcjonalnością [Szyfrowanie dysków funkcją BitLocker](#). *Rozszerzony kod PIN* umożliwia używanie innych znaków jako dodatku do znaków numerycznych: dużych i małych liter alfabetu łacińskiego, znaków specjalnych i spacji.
- Dodano funkcję [wyłączenia uwierzytelniania funkcji BitLocker dla aktualizacji systemu operacyjnego lub instalacji pakietów aktualizacyjnych](#). Instalowanie aktualizacji może wymagać ponownego uruchomienia komputera kilka razy. Aby poprawnie zainstalować aktualizacje, możesz tymczasowo wyłączyć uwierzytelnianie funkcji BitLocker i ponownie włączyć uwierzytelnianie po zainstalowaniu aktualizacji.
- Teraz możesz [ustawić czas wygaśnięcia kodu PIN lub hasła szyfrowania funkcją BitLocker](#). Jeśli hasło lub kod PIN wygaśnie, Kaspersky Endpoint Security wyświetli pytanie o nowe hasło.

7. Teraz możesz skonfigurować maksymalną liczbę prób autoryzacji klawiatury dla Ochrony przed atakami BadUSB. Jeśli [skonfigurowana liczba nieudanych prób wprowadzenia kodu autoryzacyjnego](#) zostanie osiągnięta, urządzenie USB zostanie tymczasowo zablokowane.

8. Funkcjonalność Zapory sieciowej zostanie udoskonalona:

- Teraz możesz skonfigurować zakres adresów IP dla [reguł dla pakietów modułu Zapora sieciowa](#). Możesz wprowadzić zakres adresów w formacie IPv4 lub IPv6. Na przykład: 192.168.1.1-192.168.1.100 lub 12:34::2-12:34::99.
- Teraz możesz wprowadzić nazwy DNS dla [reguł dla pakietów modułu Zapora sieciowa](#) zamiast adresów IP. Powinieneś używać nazw DNS tylko dla komputerów LAN lub wewnętrznych usług. Interakcja z usługami chmury (takimi jak Microsoft Azure) i innymi zasobami internetowymi powinna być zarządzana przez komponent Kontrola sieci.

9. Udoskonalono wyszukiwanie [reguły Kontroli sieci](#). Aby odszukać regułę dostępu do zasobu sieciowego, oprócz nazwy reguły możesz użyć adresu URL strony internetowej, nazwy użytkownika, kategorii zawartości lub typu danych.

10. Udoskonalono zadanie *Skanowanie antywirusowe*:

- Udoskonalono zadanie [Skanowanie antywirusowe](#) w czasie bezczynności. Jeśli podczas skanowania uruchomiłeś komputer ponownie, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym skanowanie zostało przerwane.
- Zoptymalizowano zadanie [Skanowanie antywirusowe](#). Domyślnie, Kaspersky Endpoint Security uruchamia skanowanie tylko wtedy, gdy komputer jest w trybie bezczynności. Możesz skonfigurować moment uruchomienia skanowania komputera we właściwościach zadania.

11. Teraz możesz ograniczyć dostęp użytkownika do danych dostarczonych przez [Monitor aktywności aplikacji](#). *Monitor aktywności aplikacji* to narzędzie służące do wyświetlania informacji o aktywności aplikacji na komputerze użytkownika w czasie rzeczywistym. Administrator może ukryć Monitor aktywności aplikacji przed użytkownikiem we właściwościach zasady aplikacji.

12. [Udoskonalono bezpieczeństwo zarządzania aplikacją za pośrednictwem interfejsu API REST](#). Teraz Kaspersky Endpoint Security sprawdza sygnaturę żądań wysyłanych za pośrednictwem API REST. Aby zarządzać programem, musisz zainstalować certyfikat identyfikacji żądania.

Aktualizacja 11.6.0

Program Kaspersky Endpoint Security 11.6.0 for Windows oferuje następujące funkcje i ulepszenia:

1. [Obsługę systemu Windows 10 21H1](#). Więcej informacji na temat obsługi systemu operacyjnego Microsoft Windows 10 można znaleźć w [Bazie wiedzy na stronie działu pomocy technicznej](#).
2. [Dodano komponent Managed Detection and Response](#). Ten komponent upraszcza interakcję z rozwiązaniem znanym jako Kaspersky Managed Detection and Response. Kaspersky Managed Detection and Response (MDR) oferuje całodobową ochronę przed rosnącą liczbą zagrożeń zdolnych do omijania zautomatyzowanych mechanizmów ochrony dla organizacji, które mają ciężki moment na znalezienie wysoko wykwalifikowanych ekspertów lub którzy posiadają ograniczone wewnętrzne zasoby. Szczegółowe informacje dotyczące sposobu działania rozwiązania można znaleźć w pomocy do Kaspersky Managed Detection and Response.
3. [Kaspersky Endpoint Agent](#), który jest zawarty w pakiecie dystrybucyjnym, został zaktualizowany do wersji 3.10. Kaspersky Endpoint Agent 3.10 oferuje nowe funkcje, rozwiązuje niektóre poprzednie problemy. Więcej informacji o aplikacji można znaleźć w dokumentacji do rozwiązań firmy Kaspersky, które obsługują Kaspersky Endpoint Agent.
4. Teraz oferuje możliwość zarządzania ochroną przed atakami, takimi jak zalewanie sieci i skanowanie portów [Ustawienia Ochrony sieci](#).
5. Dodano nową metodę tworzenia reguł sieciowych dla Zapory sieciowej. Możesz dodać [reguły do pakietów](#) i [reguły aplikacji](#) do nawiązywania połączeń, które są wyświetlane w oknie [Monitor sieci](#). Jednakże ustawienia połączenia reguły sieciowej zostaną skonfigurowane automatycznie.
6. Udoskonalono interfejs [Monitor sieci](#). Dodano informacje o aktywności sieciowej: ID procesu, która inicjuje aktywność sieciową; typ sieci (sieć lokalna lub internet); porty lokalne. Domyślnie, informacje o typie sieci są ukryte.
7. Teraz istnieje możliwość automatycznego utworzenia kont Agenta autoryzacji dla nowych użytkowników systemu Windows. Agent umożliwia użytkownikowi przeprowadzenie pełnej autoryzacji w celu uzyskania dostępu do dysków, które zostały [zaszyfrowane przy użyciu technologii Kaspersky Disk Encryption](#), i załadowania systemu operacyjnego. Aplikacja sprawdza informacje o kontach użytkowników systemu Windows na komputerze. Jeśli Kaspersky Endpoint Security wykryje konto użytkownika systemu Windows, które nie zawiera konta Agenta autoryzacji, aplikacja utworzy nowe konto do uzyskania dostępu do zaszyfrowanych dysków. To oznacza, że nie musisz [ręcznie dodawać kont Agenta autoryzacji](#) dla komputerów z już zaszyfrowanymi dyskami.
8. Teraz istnieje możliwość monitorowania procesu szyfrowania dysków w interfejsie aplikacji na komputerach użytkowników (Kaspersky Disk Encryption i BitLocker). Możesz uruchomić narzędzie Monitor szyfrowania z poziomu [okna głównego aplikacji](#).

[Aktualizacja 11.5.0](#)


Program Kaspersky Endpoint Security 11.5.0 for Windows oferuje następujące funkcje i ulepszenia:

1. [Obsługę systemu Windows 10 20H2](#). Więcej informacji na temat obsługi systemu operacyjnego Microsoft Windows 10 można znaleźć w [Bazie wiedzy na stronie działu pomocy technicznej](#).
2. Zaktualizowano [interfejs aplikacji](#). Zaktualizowano także [ikonę aplikacji w obszarze powiadomień](#), powiadomienia aplikacji i okna dialogowe.
3. Udoskonalono interfejs wtyczki webowej Kaspersky Endpoint Security dla komponentów: Kontrola aplikacji, Kontrola urządzeń i Adaptacyjna kontrola anomalii.
4. Dodano funkcjonalność importowania i eksportowania list reguł i wykluczeń w formacie XML. Format XML umożliwia edytowanie list po ich wyeksportowaniu. Możesz zarządzać listami tylko w konsoli Kaspersky Security Center Console. Do eksportowania/importowania dostępne są następujące listy:
 - [Wykrywanie zachowań \(lista wykluczeń\)](#).
 - [Ochrona WWW \(lista zaufanych adresów internetowych\)](#).
 - [Ochrona poczty \(lista rozszerzeń filtra załącznika\)](#).
 - [Ochrona sieci \(lista wykluczeń\)](#).
 - [Zapora sieciowa \(lista reguł dla pakietów sieciowych\)](#).
 - [Kontrola aplikacji \(lista reguł\)](#).
 - [Kontrola sieci \(lista reguł\)](#).
 - [Monitorowanie portu sieciowego \(listy portów i aplikacji monitorowanych przez Kaspersky Endpoint Security\)](#).
 - [Kaspersky Disk Encryption \(lista wykluczeń\)](#).
 - [Szyfrowanie nośników wymiennych \(lista reguł\)](#).
5. Informacje o sumie kontrolnej MD5 obiektu, który został dodany do [raportu dotyczącego wykrywania zagrożeń](#). W poprzednich wersjach aplikacji program Kaspersky Endpoint Security wyświetlił tylko sumę kontrolną SHA256 obiektu.
6. Dodano możliwość [przypisania priorytetu dla reguł dostępu do urządzenia](#) w ustawieniach Kontroli urządzeń. Przypisanie priorytetu umożliwia bardziej elastyczną konfigurację dostępu użytkownika do urządzeń. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 0 dla grupy administratorów oraz przypisz priorytet 1 dla grupy Każdy. Możesz skonfigurować priorytet tylko dla urządzeń, które mają system plików. To obejmuje dyski twarde, nośniki wymienne, napędy dyskietek, płyty CD/DVD oraz urządzenia przenośne (MTP).
7. Dodano nową funkcjonalność:
 - [Zarządzaj powiadomieniami audio](#).
 - Uwzględnienie kosztów połączenia Kaspersky Endpoint Security ogranicza własny ruch sieciowy, jeśli połączenie z internetem jest ograniczone (na przykład, za pośrednictwem połączenia mobilnego).

- [Zarządzaj ustawieniami Kaspersky Endpoint Security za pośrednictwem zaufanych aplikacji do zdalnej administracji](#) (np. TeamViewer, LogMeln Pro i Remotely Anywhere). Możesz użyć aplikacji do zdalnej administracji, aby uruchomić Kaspersky Endpoint Security i zarządzać ustawieniami w interfejsie aplikacji.
 - [Zarządzaj ustawieniami skanowania bezpiecznego ruchu sieciowego w Firefox i Thunderbird](#). Możesz wybrać magazyn certyfikatów, który będzie używany przez firmę Mozilla: magazyn certyfikatów systemu Windows lub magazyn certyfikatów aplikacji Mozilla. Ta funkcjonalność jest dostępna tylko dla komputerów, na których nie jest zastosowana zasada. Jeśli zasada jest stosowana na komputerze, Kaspersky Endpoint Security automatycznie włącza korzystanie z magazynu certyfikatów systemu Windows w Firefox i Thunderbird.
8. Dodana możliwość [konfigurowania trybu skanowania bezpiecznego ruchu sieciowego](#): zawsze skanuje ruch sieciowy nawet wtedy, gdy składniki ochrony są wyłączone lub skanuje ruch sieciowy po żądaniu od składników ochrony.
9. Poprawiono procedurę [usuwania informacji z raportów](#). Użytkownik może tylko usunąć wszystkie raporty. W poprzednich wersjach aplikacji użytkownik mógł wybrać określone składniki aplikacji, których informacje zostałyby usunięte z raportów.
10. Poprawiono procedurę [importowania pliku konfiguracyjnego zawierającego ustawienia Kaspersky Endpoint Security](#), a także poprawioną procedurę [przywrócenia ustawień aplikacji](#). Przed zaimportowaniem lub przywróceniem program Kaspersky Endpoint Security wyświetla tylko ostrzeżenie. W poprzednich wersjach aplikacji można było przejrzeć wartości nowych ustawień przed ich zastosowaniem.
11. Uproszczono [procedurę przywracania dostępu do dysku, który został zaszyfrowany przy użyciu funkcji BitLocker](#). Po zakończeniu procedury odzyskiwania dostępu, Kaspersky Endpoint Security wyświetli pytanie o ustawienie nowego hasła lub kodu PIN. Po ustawieniu nowego hasła, funkcja BitLocker zaszyfruje dysk. W poprzedniej wersji aplikacji użytkownik musiał ręcznie zresetować hasło w ustawieniach funkcji BitLocker.
12. Użytkownicy mają teraz możliwość utworzenia swojej własnej lokalnej [strefy zaufanej](#) dla określonego komputera. W ten sposób użytkownicy mogą utworzyć swoje własne lokalne listy [wykluczeń](#) i [zaufanych aplikacji](#) jako dodatek do ogólnej strefy zaufanej w zasadzie. Administrator może zezwolić na lub zablokować użycie lokalnych wykluczeń lub lokalnych zaufanych aplikacji. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.
13. Dodano możliwość [wprowadzenia poleceń we właściwościach zaufanych aplikacji](#). Komentarze pomagają uproszczyć wyszukiwanie i sortowanie zaufanych aplikacji.
14. [Zarządzanie aplikacją za pośrednictwem interfejsu API REST](#):
- Istnieje możliwość skonfigurowania ustawień rozszerzenia Ochrony poczty dla programu Outlook.
 - Zabronione jest wyłączenie wykrywania wirusów, robaków i programów typu trojan.

[Aktualizacja 11.4.0](#)

Program Kaspersky Endpoint Security 11.4.0 for Windows oferuje następujące funkcje i ulepszenia:







1. Nowy projekt [ikony aplikacji w obszarze powiadomień paska zadań](#). Nowa ikona  jest teraz wyświetlana zamiast starej ikony . Jeśli użytkownik jest zobowiązany do wykonania czynności (na przykład, uruchomienia ponownie komputera po aktualizacji aplikacji), ikona zmieni się na . Jeśli składniki ochrony aplikacji są wyłączone lub działają nieprawidłowo, ikona zmieni się na  lub . Po najechaniu kursorem na ikonę, Kaspersky Endpoint Security wyświetli opis problemu w ochronie komputera.
2. Kaspersky Endpoint Agent, który jest zawarty w pakiecie dystrybucyjnym, został zaktualizowany do wersji 3.9. Kaspersky Endpoint Agent 3.9 obsługuje integrację z nowymi rozwiązaniami Kaspersky. Więcej informacji o aplikacji można znaleźć w dokumentacji do rozwiązań firmy Kaspersky, które obsługują Kaspersky Endpoint Agent.
3. Dodano stan *Nie jest obsługiwany przez licencję* dla komponentów Kaspersky Endpoint Security. Możesz wyświetlić stan komponentów, klikając przycisk **Składniki ochrony** w [oknie głównym aplikacji](#).
4. Nowe zdarzenia z [Ochrony przed exploitami](#) zostały dodane do [raportów](#).
5. Sterowniki [technologii szyfrowania Kaspersky Disk Encryption](#) są teraz automatycznie dodawane do środowiska odzyskiwania systemu Windows (WinRE) po uruchomieniu szyfrowania dysku. Poprzednia wersja Kaspersky Endpoint Security dodawała sterowniki podczas instalowania aplikacji. Dodawanie sterowników do WinRE może udoskonalić stabilność aplikacji podczas odzyskiwania systemu operacyjnego na komputerach chronionych przez technologię Kaspersky Disk Encryption.

Komponent Endpoint Sensor został usunięty z Kaspersky Endpoint Security. Nadal możesz skonfigurować ustawienia Endpoint Sensor w zasadzie, pod warunkiem, że na komputerze jest zainstalowany Kaspersky Endpoint Security w wersji od 11.0.0 do 11.3.0.

Kaspersky Endpoint Security for Windows

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


Technologie wykrywania zagrożeń

<p> Uczenie maszynowe</p> <p>Kaspersky Endpoint Security używa modeli opartych o uczenie maszynowe. Model został opracowany przez ekspertów z firmy Kaspersky. Model jest cały czas uzupełnianymi danymi zagrożeń z KSN (uczenie modelu).</p> <p> Analiza w chmurze</p> <p>Kaspersky Endpoint Security pobiera dane zagrożeń z Kaspersky Security Network. <i>Kaspersky Security Network (KSN)</i> jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania.</p> <p> Analiza ekspercka</p> <p>Kaspersky Endpoint Security wykorzystuje dane zagrożeń pobrane przez analityków wirusów Kaspersky. Analitycy wirusów oceniają, czy reputacja obiektów nie może zostać określona automatycznie.</p>	<p> Analiza zachowań</p> <p>Kaspersky Endpoint Security analizuje aktywność obiektu w czasie rzeczywistym.</p> <p> Analiza automatyczna</p> <p>Kaspersky Endpoint Security pobiera dane z systemu automatycznej analizy obiektów. System przetwarza wszystkie obiekty, które są wysyłane do Kaspersky. Następnie system określa reputację obiektu i dodaje dane do antywirusowych baz danych. Jeśli system nie może określić reputacji obiektu, system pyta analityków wirusów z Kaspersky.</p> <p> Kaspersky Sandbox</p> <p>Kaspersky Endpoint Security przetwarza obiekt na maszynie wirtualnej. Kaspersky Sandbox analizuje zachowanie obiektu i podejmuje decyzję odnośnie jego reputacji. Ta technologia jest dostępna tylko wtedy, gdy używasz rozwiązania Kaspersky Sandbox.</p>
---	--

Drzewo wyboru

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

Drzewo wyboru

Sekcja	Składnik
<p>Podstawowa ochrona przed zagrożeniami</p> <p></p>	<p>Ochrona plików</p> <p>Komponent Ochrona plików umożliwia uniknięcie infekcji systemu plików komputera. Domyślnie, składnik Ochrona plików na stałe znajduje się w pamięci RAM komputera. Składnik skanuje pliki na wszystkich dyskach komputera, a także na podłączonych dyskach. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i analizy heurystycznej.</p> <p>Ochrona WWW</p>

Komponent Ochrona WWW zapobiega pobieraniu szkodliwych plików z internetu, a także blokuje szkodliwe i phishingowe strony internetowe. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, [usługi w chmurze Kaspersky Security Network](#) i analizy heurystycznej.

Ochrona poczty

Ochrona poczty skanuje załączniki odbieranych i wysyłanych wiadomości e-mail w poszukiwaniu wirusów i innych zagrożeń. Komponent skanuje również wiadomości w poszukiwaniu szkodliwych i phishingowych odnośników. Domyślnie, składnik Ochrona poczty na stałe znajduje się w pamięci RAM komputera i skanuje wszystkie wiadomości otrzymane lub wysłane za pomocą protokołów POP3, SMTP, IMAP lub NNTP lub klienta poczty Microsoft Office Outlook (MAPI). Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, [usługi w chmurze Kaspersky Security Network](#) i analizy heurystycznej.

Ochrona sieci

Moduł Ochrona sieci bada przychodzący ruch sieciowy pod kątem aktywności typowych dla ataków sieciowych. Jeśli Kaspersky Endpoint Security wykryje próbę ataku sieciowego na komputerze użytkownika, zablokuje połączenie sieciowe z komputerem atakującym. Opisy znanych typów ataków sieciowych oraz sposoby ich zwalczania znajdują się w bazach danych programu Kaspersky Endpoint Security. Lista ataków sieciowych, wykrywanych przez komponent Ochrona sieci, jest uaktualniana podczas [aktualizacji baz danych i modułów aplikacji](#).

Zapora sieciowa

Zapora sieciowa blokuje nieautoryzowane połączenia z komputerem podczas pracy w internecie lub sieci lokalnej. Zapora sieciowa kontroluje również aktywność sieciową aplikacji na komputerze. Pozwala to chronić korporacyjną sieć LAN przed kradzieżą tożsamości i innymi atakami. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i predefiniowanych *reguł sieciowych*.

Ochrona przed atakami BadUSB

Komponent Ochrona przed atakami BadUSB zapobiega podłączeniu do komputera zainfekowanych urządzeń USB emulujących klawiaturę.

Ochrona AMSI

Komponent Ochrona AMSI jest przeznaczony do obsługi Antimalware Scan Interface firmy Microsoft. *Antimalware Scan Interface (AMSI)* umożliwia aplikacjom firm trzecich z obsługą AMSI wysyłanie obiektów (na przykład, skryptów PowerShell) do Kaspersky Endpoint Security w celu przeprowadzenia dodatkowego skanowania i otrzymania wyników ze skanowania tych obiektów.

Zaawansowana ochrona przed zagrożeniami



Kaspersky Security Network

Kaspersky Security Network (KSN) jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Endpoint Security na nowe zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. Jeśli uczestniczysz w Kaspersky Security Network, usługi KSN zapewniają Kaspersky Endpoint Security informacje o kategorii i reputacji przeskanowanych plików, a także informacje o reputacji przeskanowanych adresów internetowych.

Wykrywanie zachowań

Komponent Wykrywanie zachowań gromadzi dane na temat działań aplikacji na komputerze i dostarcza te informacje innym składnikom ochrony w celu udoskonalenia ich działania. Komponent Wykrywanie zachowań używa sygnatur strumieni zachowań (BSS) dla aplikacji. Jeśli aktywność aplikacji odpowiada sygnaturze strumienia zachowań, Kaspersky Endpoint Security wykona wybrane działanie. Funkcjonalność Kaspersky Endpoint Security oparta na sygnaturach strumieni zachowań zapewnia ochronę proaktywną komputera.

Ochrona przed exploitami

Komponent Ochrona przed exploitami wykrywa kod programu, który wykorzystuje luki na komputerze, aby użyć uprawnień administratora lub wykonać szkodliwe aktywności. Na przykład, exploit może używać ataku typu buffer overflow (przepełnienie bufora). Aby to zrobić, exploit wysyła dużą ilość danych do aplikacji zawierającej lukę. Podczas przetwarzania tych danych aplikacja zawierająca lukę wykona szkodliwy kod. W wyniku tego ataku exploit może uruchomić nieautoryzowaną instalację szkodliwego programu. Po wykryciu, że próba uruchomienia pliku wykonywalnego z aplikacji zawierającej luki nie została zainicjowana przez użytkownika, Kaspersky Endpoint Security zablokuje uruchomienie tego pliku lub poinformuje użytkownika.

Ochrona przed włamaniami

Ochrona przed włamaniami uniemożliwia aplikacjom wykonywanie działań niebezpiecznych dla systemu operacyjnego i zapewnia kontrolę dostępu do zasobów systemu operacyjnego i danych osobowych. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network.

Silnik korygujący

Silnik korygujący umożliwia Kaspersky Endpoint Security wycofanie działań, które zostały wykonane przez szkodliwe oprogramowanie w systemie operacyjnym.

Kontrola zabezpieczeń



Kontrola aplikacji

Kontrola aplikacji zarządza uruchamianiem aplikacji na komputerach użytkowników. Pozwala to na wdrożenie polityki bezpieczeństwa firmy podczas korzystania z aplikacji. Kontrola aplikacji zmniejsza także ryzyko infekcji komputera poprzez ograniczenie dostępu do aplikacji.

Kontrola urządzeń

Kontrola urządzeń zarządza dostępem użytkownika do urządzeń, które są instalowane na komputerze lub są podłączone do komputera (na przykład: dyski twarde, kamery lub moduły Wi-Fi). Umożliwia to ochronę komputera przed infekcją, gdy takie urządzenia są podłączone, oraz zapobieganie utracie lub wyciekowi danych.

Kontrola sieci

Kontrola sieci zarządza dostępem użytkowników zasobów sieciowych. Pomaga to zmniejszyć ruch sieciowy i nieodpowiednie dysponowanie czasem pracy. Gdy użytkownik próbuje otworzyć stronę internetową ograniczoną przez Kontrolę sieci, Kaspersky Endpoint Security zablokuje dostęp lub wyświetli ostrzeżenie.

Adaptacyjna kontrola anomalii

Komponent Adaptacyjna kontrola anomalii monitoruje i blokuje działania, które nie są typowe dla komputerów w sieci firmowej. Adaptacyjna kontrola anomalii wykorzystuje zestaw reguł do śledzenia nietypowych zachowań (na przykład, reguła *Uruchom Microsoft PowerShell z aplikacji biurowych*). Reguły są tworzone przez specjalistów z Kaspersky w oparciu o typowe scenariusze złośliwej aktywności. Można skonfigurować, w jaki sposób Adaptacyjna kontrola aplikacji obsługuje każdą regułę i, na przykład, zezwolić na wykonywanie skryptów PowerShell, które automatyzują określone zadania przepływu pracy. Kaspersky Endpoint Security aktualizuje zestaw reguł wraz z bazami danych aplikacji.

Szyfrowanie

Szyfrowanie plików



Komponent umożliwia utworzenie reguł szyfrowania plików. Możesz wybrać predefiniowane foldery do szyfrowania, ręcznie wybrać folder lub wybrać pojedyncze pliki według rozszerzenia.

Szyfrowanie całego dysku

Komponent umożliwia szyfrowanie dysku twardego przy użyciu funkcji Kaspersky Disk Encryption lub Szyfrowanie dysków funkcją BitLocker.

Szyfrowanie nośników wymiennych

Komponent umożliwia ochronę danych na dyskach wymiennych. Możesz użyć funkcji Szyfrowanie całego dysku (FDE) lub Szyfrowanie plików (FLE).

Detection and Response



Endpoint Detection and Response

Wbudowany agent dla rozwiązania Kaspersky Endpoint Detection and Response Optimum (zwany dalej „EDR Optimum”). *Kaspersky Endpoint Detection and Response Optimum* to rozwiązanie do ochrony infrastruktury IT organizacji przed zaawansowanymi cyberzagrożeniami. Funkcjonalność rozwiązania łączy automatyczne wykrywanie zagrożeń z możliwością reagowania na te zagrożenia w celu przeciwdziałania zaawansowanym atakom, w tym nowym exploitom, oprogramowaniu ransomware, atakom bezplikowym, a także metodom z użyciem legalnych narzędzi systemowych. Więcej informacji o rozwiązaniu można znaleźć w *pomocy online dla [Kaspersky Endpoint Detection and Response Optimum](#)*.

Kaspersky Sandbox

Komponent umożliwia współdziałanie z rozwiązaniem Kaspersky Sandbox. *Rozwiązanie Kaspersky Sandbox* wykrywa i automatycznie blokuje zaawansowane zagrożenia na komputerach. Kaspersky Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Kaspersky Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Kaspersky Sandbox). Więcej informacji o rozwiązaniu można znaleźć w *pomocy dla [Kaspersky Sandbox](#)*.

Managed Detection and Response

Wbudowany agent do obsługi działania rozwiązania Kaspersky Managed Detection and Response. Rozwiązanie *Kaspersky Managed Detection and Response (MDR)* automatycznie wykrywa i analizuje incydenty naruszenia bezpieczeństwa w Twojej infrastrukturze. W tym celu MDR używa danych telemetrycznych, otrzymanych z punktów końcowych i uczenia maszynowego. MDR wysyła dane incydu do ekspertów z Kaspersky. Ekspersi mogą następnie przetworzyć incydent i, na przykład, dodać nowy wpis do antywirusowych baz danych. Zamiast tego eksperci mogą opublikować zalecenia odnośnie przetwarzania incydu i, na przykład, zasugerować odizolowanie komputera od sieci. Szczegółowe informacje dotyczące sposobu działania rozwiązania *można znaleźć w [pomocy do Kaspersky Managed Detection and Response](#)*.

Poza ochroną w czasie rzeczywistym zapewnianą przez moduły aplikacji, zalecamy regularne *skanowanie komputera* w poszukiwaniu wirusów i innych zagrożeń. Pomaga to wykluczyć możliwość rozprzestrzeniania szkodliwego oprogramowania, które nie zostało wykryte przez składniki ochrony, na przykład, ze względu na niski poziom ochrony.

Aby ochrona komputera była aktualna, musisz *zaktualizować bazy danych i moduły* aplikacji. Domyślnie aplikacja jest aktualizowana automatycznie, ale w razie konieczności możesz zawsze uruchomić aktualizację baz danych i modułów aplikacji ręcznie.

W Kaspersky Endpoint Security dostępne są następujące zadania:

- **Sprawdzanie integralności.** Kaspersky Endpoint Security sprawdza, czy moduły aplikacji w folderze instalacyjnym aplikacji nie są uszkodzone lub zmodyfikowane. Jeśli moduł aplikacji posiada nieprawidłowy podpis cyfrowy, moduł zostanie uznany za uszkodzony.

- **Pełne skanowanie.** Kaspersky Endpoint Security skanuje system operacyjny, włączając w to pamięć jądra, obiekty ładowane podczas uruchamiania systemu operacyjnego, sektory rozruchowe dysku, miejsce przechowywania kopii zapasowych systemu operacyjnego oraz wszystkie dyski twarde i wymienne.
- **Skanowanie obiektów.** Kaspersky Endpoint Security skanuje obiekty wybrane przez użytkownika.
- **Skanowanie obszarów krytycznych.** Kaspersky Endpoint Security skanuje pamięć jądra, obiekty ładowane podczas uruchamiania systemu operacyjnego i sektory rozruchowe dysku.
- **Aktualizacja.** Kaspersky Endpoint Security pobiera uaktualnienia baz danych i modułów aplikacji. Aktualizacja zapewnia ochronę komputera przed najnowszymi wirusami i innymi zagrożeniami.
- **Wycofanie ostatniej aktualizacji.** Kaspersky Endpoint Security wycofuje ostatnią aktualizację baz danych i modułów. Umożliwi to w razie czego wycofanie baz danych i modułów aplikacji do ich poprzedniej wersji, na przykład, gdy nowa wersja baz danych zawiera nieprawidłową sygnaturę powodującą, że Kaspersky Endpoint Security blokuje bezpieczną aplikację.

Funkcje usługowe aplikacji

Kaspersky Endpoint Security zawiera pewną liczbę funkcji usługowych. Służą one do utrzymywania aktualnego stanu aplikacji, rozszerzania jej funkcjonalności i pomocy użytkownikowi w pracy z aplikacją.

- **Raporty.** W trakcie działania aplikacja tworzy raporty dotyczące każdego swojego składnika. Możesz także używać raportów do śledzenia wyników zakończonych zadań. Raporty zawierają listy zdarzeń, które wystąpiły podczas działania Kaspersky Endpoint Security, oraz wszystkie działania wykonywane przez aplikację. W przypadku wystąpienia problemu, można przesłać raporty do firmy Kaspersky, gdzie specjaliści z pomocy technicznej przyjrzą się problemowi i pomogą go rozwiązać.
- **Kopia zapasowa.** Jeżeli podczas skanowania komputera w poszukiwaniu wirusów i innych zagrożeń aplikacja wykryje zainfekowane pliki, zablokuje je. Kaspersky Endpoint Security przechowuje kopie zainfekowanych i usuniętych plików w *Kopii zapasowej*. Kaspersky Endpoint Security przenosi pliki, które z jakiegoś powodu nie zostały przetworzone, na *listę aktywnych zagrożeń*. Możesz skanować pliki, przywracać pliki do ich oryginalnych folderów i czyścić miejsca przechowywania danych.
- **Powiadomienia.** Usługa powiadamiania pomaga użytkownikowi w śledzeniu zdarzeń, które wpływają na stan ochrony komputera i działanie Kaspersky Endpoint Security. Powiadomienia mogą być wyświetlane na ekranie lub przesyłane pocztą elektroniczną.
- **Kaspersky Security Network.** Uczestnictwo użytkownika w Kaspersky Security Network zwiększa efektywność ochrony komputera dzięki użyciu w czasie rzeczywistym informacji o reputacji plików, zasobach sieciowych i oprogramowaniu, otrzymanych od użytkowników z całego świata.
- **Licencja.** Zakup licencji odblokowuje pełną funkcjonalność aplikacji, zapewnia dostęp do aktualizacji baz danych i modułów aplikacji oraz pomocy technicznej za pośrednictwem telefonu lub poczty elektronicznej w sprawach związanych z instalacją, konfiguracją i korzystaniem z aplikacji.
- **Pomoc techniczna.** Wszyscy zarejestrowani użytkownicy Kaspersky Endpoint Security mogą skontaktować się ze specjalistami z pomocy technicznej Kaspersky w celu uzyskania pomocy. Możesz wysłać zgłoszenie do działu pomocy technicznej Kaspersky poprzez portal Kaspersky CompanyAccount lub skontaktować się z pomocą techniczną telefonicznie.

Jeśli podczas działania aplikacja zwróci błędy lub zawiesi się, może zostać automatycznie uruchomiona ponownie.

Jeśli aplikacja napotka powtarzające się błędy powodujące jej awarię, wykona ona następujące działania:

1. Wyłączy funkcje kontroli i ochrony (funkcja szyfrowania pozostanie włączona).

2. Powiadomi użytkownika o wyłączeniu funkcji.

3. Podejmie próbę przywrócenia aplikacji do stanu funkcjonalności po zaktualizowaniu baz danych lub zastosowaniu uaktualnień modułów aplikacji.

Pakiet dystrybucyjny

Pakiet dystrybucyjny zawiera następujące pakiety dystrybucyjne:

- **Silne szyfrowanie (AES256)**

Ten pakiet dystrybucyjny zawiera narzędzia kryptograficzne, które implementują algorytm szyfrowania AES (Advanced Encryption Standard) o efektywnej długości klucza wynoszącej 256 bitów.

- **Uprozczone szyfrowanie (AES56)**

Ten pakiet dystrybucyjny zawiera narzędzia kryptograficzne, które implementują algorytm szyfrowania AES o efektywnej długości klucza wynoszącej 56 bitów.

Każdy pakiet dystrybucyjny zawiera następujące pliki:

kes_win.msi	Pakiet instalacyjny Kaspersky Endpoint Security.
setup_kes.exe	Pliki wymagane do instalacji aplikacji przy użyciu jednej z dostępnych metod.
kes_win.kud	Plik do tworzenia pakietów instalacyjnych dla Kaspersky Endpoint Security .
klcfginst.msi	Pakiet instalacyjny wtyczki zarządzającej Kaspersky Endpoint Security dla Kaspersky Security Center.
bases.cab	Pliki pakietu aktualizacyjnego, które są używane podczas instalacji.
cleaner.cab	Pliki do usuwania niekompatybilnego oprogramowania.
incompatible.txt	Plik zawierający listę niekompatybilnego oprogramowania.
ksn_<ID_języka>.txt	Plik, w którym możesz przeczytać warunki uczestnictwa w Kaspersky Security Network.
license.txt	Plik, w którym możesz przeczytać Umowę licencyjną i Politykę prywatności.
installer.ini	Plik, który zawiera wewnętrzne ustawienia pakietu dystrybucyjnego.
endpointagent.msi	Pakiet instalacyjny dla Kaspersky Endpoint Agent , który jest wymagany do integracji z innymi rozwiązaniami Kaspersky (na przykład: Kaspersky Sandbox).
NDP<wersja>-<właściwości pakietu>	Pakiet instalacyjny Microsoft .NET Framework.
keswin_web_plugin.zip	Archiwum zawierające pliki wymagane do zainstalowania wtyczki webowej Kaspersky Endpoint Security .

Nie jest zalecane zmienianie wartości tych ustawień. Jeśli chcesz zmienić opcje instalacji, użyj [pliku setup.ini](#).

Wymagania sprzętowe i programowe

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

Minimalne wymagania ogólne:

- 2 GB wolnego miejsca na dysku twardym
- Procesor:
 - Stacja robocza: 1 GHz
 - Serwer: 1.4 GHz
 - Obsługa zestawu instrukcji SSE2
- Pamięć RAM:
 - Stacja robocza (x86): 1 GB
 - Stacja robocza (x64): 2 GB
 - Serwer: 2 GB
- Microsoft .NET Framework 4.0 lub nowszy

Obsługiwane systemy operacyjne dla stacji roboczych:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 lub nowszy;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows 11.

Algorytm podpisu modułu SHA-1 jest przestarzały według firmy Microsoft. Aktualizacja KB4474419 jest wymagana do pomyślnej instalacji Kaspersky Endpoint Security na komputerze działającym pod systemem operacyjnym Microsoft Windows 7. Więcej informacji o tej stronie można znaleźć na [stronie internetowej pomocy technicznej firmy Microsoft](#).

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

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

Obsługiwane systemy operacyjne dla serwerów:

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

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

- Windows MultiPoint Server 2011 (64-bitowy);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 lub nowszy;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Algorytm podpisu modułu SHA-1 jest przestarzały według firmy Microsoft. Aktualizacja KB4474419 jest wymagana do pomyślnej instalacji Kaspersky Endpoint Security na komputerze działającym pod systemem operacyjnym Microsoft Windows Server 2008 R2. Więcej informacji o tej stronie można znaleźć na [stronie internetowej pomocy technicznej firmy Microsoft](#).

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

Więcej informacji na temat obsługi systemu operacyjnego Microsoft Windows 2022 można znaleźć w [Bazie wiedzy na stronie działu pomocy technicznej](#).

Obsługiwane typy serwerów terminalowych:

- Microsoft Remote Desktop Services oparty na Windows Server 2008 R2 SP1;
- Microsoft Remote Desktop Services oparty na Windows Server 2012;
- Microsoft Remote Desktop Services oparty na Windows Server 2012 R2;
- Microsoft Remote Desktop Services oparty na Windows Server 2016;
- Microsoft Remote Desktop Services oparty na Windows Server 2019.

Obsługiwane platformy wirtualne:

- VMware Workstation 16.1.1 Pro;
- VMware ESXi 7.0 Update 2a;
- Microsoft Hyper-V Server 2019;
- Citrix Virtual Apps and Desktops 7 2103;

- Citrix Provisioning 2012;
- Citrix Hypervisor 8.2 LTSR.

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

- Kaspersky Security Center 11;
- Kaspersky Security Center 12;
- Kaspersky Security Center 12 z poprawką A;
- Kaspersky Security Center 12 z poprawką B;
- Kaspersky Security Center 13;
- Kaspersky Security Center 13.1;
- Kaspersky Security Center 13.2.

Porównanie dostępnych funkcji aplikacji w zależności od typu systemu operacyjnego

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

Porównanie funkcji Kaspersky Endpoint Security

Funkcja	Stacja robocza	Serwer
Zaawansowana ochrona przed zagrożeniami		
Kaspersky Security Network	✓	✓
Wykrywanie zachowań	✓	✓
Ochrona przed exploitami	✓	✓
Ochrona przed włamaniami	✓	–
Silnik korygujący	✓	✓
Podstawowa ochrona przed zagrożeniami		
Ochrona plików	✓	✓
Ochrona WWW	✓	–
Ochrona poczty	✓	–
Zapora sieciowa	✓	✓
Ochrona sieci	✓	✓
Ochrona przed atakami BadUSB	✓	✓
Ochrona AMSI	✓	✓
Kontrola zabezpieczeń		

Kontrola aplikacji	✓	✓
Kontrola urządzeń	✓	–
Kontrola sieci	✓	–
Adaptacyjna kontrola anomalii	✓	–
Szyfrowanie danych		
Kaspersky Disk Encryption	✓	–
Szyfrowanie dysków funkcją BitLocker	✓	✓
Szyfrowanie plików	✓	–
Szyfrowanie nośników wymiennych	✓	–
Detection and Response		
Kaspersky Endpoint Agent	✓	✓
Endpoint Detection and Response Optimum	✓	✓
Kaspersky Sandbox	✓	✓
Managed Detection and Response	✓	✓

Porównanie funkcji aplikacji w zależności od narzędzi do zarządzania

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

Możesz zarządzać aplikacją za pomocą następujących konsol Kaspersky Security Center:

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

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

Porównanie funkcji Kaspersky Endpoint Security

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

Ochrona przed exploitami	✓	✓	✓
Ochrona przed włamaniami	✓	✓	✓
Silnik korygujący	✓	✓	✓
Podstawowa ochrona przed zagrożeniami			
Ochrona plików	✓	✓	✓
Ochrona WWW	✓	✓	✓
Ochrona poczty	✓	✓	✓
Zapora sieciowa	✓	✓	✓
Ochrona sieci	✓	✓	✓
Ochrona przed atakami BadUSB	✓	✓	✓
Managed Detection and Response	✓	✓	✓
Ochrona AMSI	✓	✓	✓
Kontrola zabezpieczeń			
Kontrola aplikacji	✓	✓	✓
Kontrola urządzeń	✓	✓	✓
Kontrola sieci	✓	✓	✓
Adaptacyjna kontrola anomalii	✓	✓	✓
Szyfrowanie danych			
Kaspersky Disk Encryption	✓	✓	–
Szyfrowanie dysków funkcją BitLocker	✓	✓	✓
Szyfrowanie plików	✓	✓	–
Szyfrowanie nośników wymiennych	✓	✓	–
Detection and Response			
Kaspersky Endpoint Agent	✓	✓	✓
Endpoint Detection and Response Optimum (EDR)	–	✓	✓
Kaspersky Sandbox	–	✓	✓
Managed Detection and Response	✓	✓	✓
Zadania			
Dodawanie klucza	✓	✓	✓
Zmiana składników aplikacji	✓	✓	✓
Inwentaryzacja	✓	✓	✓
Aktualizacja	✓	✓	✓
Wycofywanie aktualizacji	✓	✓	✓
Skanowanie antywirusowe	✓	✓	✓
Sprawdzanie integralności	✓	✓	–
Wyczyść dane	✓	✓	✓

Zarządzanie kontami Agenta autoryzacji (Kaspersky Disk Encryption)	✓	✓	–
Skanowanie IoC (EDR)	–	✓	✓
Przenieś plik do Kwarantanny (EDR)	–	✓	✓
Uzyskaj plik (EDR)	–	✓	✓
Usuń plik (EDR)	–	✓	✓
Rozpoczęcie procesu (EDR)	–	✓	✓
Zakończ proces (EDR)	–	✓	✓

Kompatybilność z innymi aplikacjami

Przed instalacją Kaspersky Endpoint Security sprawdzi komputer na obecność aplikacji firmy Kaspersky. Aplikacja sprawdza także komputer pod kątem niekompatybilnego oprogramowania. Lista niekompatybilnego oprogramowania jest dostępna w pliku incompatible.txt, który znajduje się w [pakiecie dystrybucyjnym](#).

 [POBIERZ PLIK INCOMPATIBLE.TXT](#) 

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

- Kaspersky Small Office Security.
- Kaspersky Internet Security.
- Kaspersky Anti-Virus.
- Kaspersky Total Security.
- Kaspersky Safe Kids.
- Kaspersky Free.
- Kaspersky Anti-Ransomware Tool.
- Kaspersky Anti Targeted Attack Platform (w tym komponent Endpoint Sensor).
- Kaspersky Sandbox (w tym Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (w tym składnik Endpoint Sensor).

Jeśli komponent Endpoint Agent został zainstalowany na komputerze za pomocą narzędzi do wdrażania innych aplikacji firmy Kaspersky, komponent zostanie automatycznie usunięty podczas instalacji Kaspersky Endpoint Security. Kaspersky Endpoint Security może również zawierać składnik Endpoint Sensor/Kaspersky Endpoint Agent, jeśli wybrałeś Endpoint Agent na liście składników aplikacji.

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

- Kaspersky Security for Windows Server.
- Kaspersky Embedded Systems Security.

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

Instalowanie i dezinstalowanie aplikacji

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

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

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

1. Ustawienia uzyskane z pliku [setup.ini](#).
2. Ustawienia uzyskane z pliku installer.ini.
3. Ustawienia uzyskane z [wiersza poleceń](#).

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

Wdrożenie za pośrednictwem Kaspersky Security Center

Kaspersky Endpoint Security może zostać zainstalowany na komputerach w obrębie sieci korporacyjnej na kilka sposobów. Możesz użyć scenariusza zdalnej instalacji najodpowiedniejszego dla Twojej organizacji lub połączyć kilka scenariuszy zdalnej instalacji. Kaspersky Security Center obsługuje następujące główne metody zdalnej instalacji:

- Instalowanie aplikacji przy użyciu Kreatora wdrażania ochrony.
[Standardowa metoda instalacji](#) jest odpowiednia, jeśli jesteś usatysfakcjonowany domyślnymi ustawieniami Kaspersky Endpoint Security, a Twoja organizacja posiada prostą infrastrukturę, która nie wymaga specjalnych konfiguracji.
- Instalowanie aplikacji przy pomocy zadania zdalnej instalacji.
Uniwersalna metoda instalacji, która umożliwia skonfigurowanie ustawień Kaspersky Endpoint Security i elastyczne zarządzanie zadaniami zdalnej instalacji. Instalacja Kaspersky Endpoint Security obejmuje następujące kroki:
 1. [Tworzenie pakietu instalacyjnego](#).
 2. [Tworzenie zadania zdalnej instalacji](#).

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

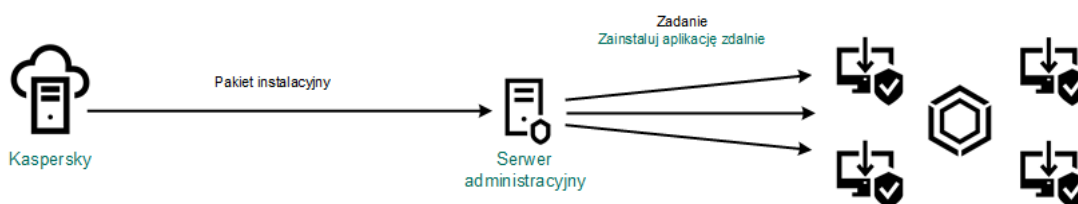
Standardowa instalacja aplikacji

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

1. Wybieranie pakietu instalacyjnego Kaspersky Endpoint Security.

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

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



Zdalna instalacja Kaspersky Endpoint Security

[Jak uruchomić Kreatora wdrażania ochrony w Konsoli administracyjnej \(MMC\)?](#)

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Dodatkowe** → **Instalacja zdalna**.
2. Kliknij odnośnik **Wdróż pakiet instalacyjny na zarządzanych urządzeniach (stacjach roboczych)**.

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

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

Krok 1. Wybieranie pakietu instalacyjnego

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

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

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

Krok 2. Wybieranie urządzeń do instalacji

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

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

Krok 3. Określanie ustawień zadania zdalnej instalacji

Skonfiguruj następujące dodatkowe ustawienia aplikacji:

- **Wymuś pobranie pakietu instalacyjnego.** Wybierz metodę instalacji aplikacji:
 - **Przy użyciu Agenta sieciowego.** Jeśli Agent sieciowy nie został zainstalowany na komputerze, w pierwszej kolejności Agent sieciowy zostanie zainstalowany przy użyciu narzędzi systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie zainstalowany przez narzędzia Agenta sieciowego.
 - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji.** Pakiet instalacyjny jest dostarczany na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty

dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji [znajdziesz w pomocy do Kaspersky Security Center](#).

- **Przy użyciu zasobów systemu operacyjnego przez serwer administracyjny.** Pliki zostaną dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.
- **Zachowanie dla urządzeń zarządzanych poprzez inne Serwery administracyjne.** Wybierz metodę instalacji Kaspersky Endpoint Security. Jeśli w sieci jest zainstalowanych więcej niż jeden Serwer administracyjny, te Serwery administracyjne mogą widzieć te same komputery klienckie. Może to spowodować, na przykład, zdalne zainstalowanie aplikacji na tym samym komputerze kilka razy poprzez różne Serwery administracyjne lub inne konflikty.
- **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana.** Odznacz to pole, jeśli chcesz, na przykład, zainstalować wcześniejszą wersję aplikacji.
- **Przypisz instalację Agenta sieciowego do zasad grupy Active Directory.** Ręczna instalacja Agenta sieciowego przy użyciu zasobów Active Directory. Aby zainstalować Agenta sieciowego, zadanie zdalnej instalacji musi być uruchomione z uprawnieniami administratora domeny.

Krok 4. Wybieranie klucza licencyjnego

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

Krok 5. Wybieranie ustawienia ponownego uruchomienia systemu operacyjnego

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

Krok 6. Usuwanie niekompatybilnych aplikacji przed zainstalowaniem aplikacji

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

Krok 7. Wybieranie konta w celu uzyskania dostępu do urządzeń

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

Krok 8. Uruchamianie instalacji

Zakończ działanie Kreatora. W razie potrzeby zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

[Jak uruchomić Kreatora wdrażania ochrony w Web Console i Cloud Console?](#) 

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

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

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

Krok 1. Wybieranie pakietu instalacyjnego

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

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

Krok 2. Wybieranie klucza licencyjnego

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

Krok 3. Wybieranie Agenta sieciowego

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

Krok 4. Wybieranie urządzeń do instalacji

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

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

Krok 5. Konfigurowanie ustawień zaawansowanych

Skonfiguruj następujące dodatkowe ustawienia aplikacji:

- **Wymuś pobranie pakietu instalacyjnego.** Wybieranie metody instalacji aplikacji:
 - **Przy użyciu Agentu sieciowego.** Jeśli Agent sieciowy nie został zainstalowany na komputerze, w pierwszej kolejności Agent sieciowy zostanie zainstalowany przy użyciu narzędzi systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie zainstalowany przez narzędzia Agentu sieciowego.
 - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji.** Pakiet instalacyjny jest dostarczany na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji [znajdziesz w pomocy do Kaspersky Security Center](#).
 - **Przy użyciu zasobów systemu operacyjnego przez serwer administracyjny.** Pliki zostaną dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agentu sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.
- **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana.** Odznacz to pole, jeśli chcesz, na przykład, zainstalować wcześniejszą wersję aplikacji.
- **Przypisz pakiet instalacyjny do zasad grupy Active Directory.** Kaspersky Endpoint Security jest instalowany przy użyciu Agentu sieciowego lub ręcznie przy użyciu Active Directory. Aby zainstalować Agentu sieciowego, zadanie zdalnej instalacji musi być uruchomione z uprawnieniami administratora domeny.

Krok 6. Wybieranie ustawienia ponownego uruchomienia systemu operacyjnego

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

Krok 7. Usuwanie niekompatybilnych aplikacji przed zainstalowaniem aplikacji

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

Krok 8. Przypisywanie do grupy administracyjnej

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

Krok 9. Wybieranie konta w celu uzyskania dostępu do urządzeń

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

Krok 10. Uruchamianie instalacji

Zakończ działanie Kreatora. W razie potrzeby zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Tworzenie pakietu instalacyjnego

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

[Jak utworzyć pakiet instalacyjny w Konsoli administracyjnej \(MMC\)?](#) 

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Dodatkowe** → **Instalacja zdalna** → **Pakiety instalacyjne**.

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

2. Kliknij przycisk **Utwórz pakiet instalacyjny**.

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

Krok 1. Wybieranie typu pakietu instalacyjnego

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

Krok 2. Określanie nazwy pakietu instalacyjnego

Wprowadź nazwę pakietu instalacyjnego, na przykład: Kaspersky Endpoint Security for Windows 11.7.0.

Krok 3. Wybieranie pakietu dystrybucyjnego do zainstalowania

Kliknij **Przeglądaj** i wybierz plik `kes_win.kud`, który jest zawarty w [pakiecie dystrybucyjnym](#).

W razie potrzeby zaktualizuj antywirusowe bazy danych w pakiecie instalacyjnym, korzystając z pola **Kopiuj aktualizacje z repozytorium do pakietu instalacyjnego**.

Krok 4. Umowa licencyjna użytkownika końcowego i Polityka prywatności

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

Pakiet instalacyjny zostanie utworzony i dodany do Kaspersky Security Center. Korzystając z pakietu instalacyjnego, możesz zainstalować Kaspersky Endpoint Security na komputerach w sieci firmowej lub zaktualizować wersję aplikacji. W ustawieniach pakietu instalacyjnego możesz także utworzyć składniki aplikacji i skonfigurować ustawienia instalacji aplikacji (patrz tabela poniżej). Pakiet instalacyjny zawiera antywirusowe bazy danych z repozytorium Serwera administracyjnego. Możesz [zaktualizować bazy danych w pakiecie instalacyjnym](#), aby zmniejszyć ruch sieciowy podczas aktualizacji baz danych po zainstalowaniu Kaspersky Endpoint Security.

[Jak utworzyć pakiet instalacyjny w Web Console i Cloud Console?](#) 

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

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

2. Kliknij przycisk **Dodaj**.

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

Krok 1. Wybieranie typu pakietu instalacyjnego

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

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

Możliwe jest także utworzenie pakietu instalacyjnego z pliku.

Krok 2. Pakiety instalacyjne

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

Pakiet instalacyjny zostanie utworzony i dodany do Kaspersky Security Center. Korzystając z pakietu instalacyjnego, możesz zainstalować Kaspersky Endpoint Security na komputerach w sieci firmowej lub zaktualizować wersję aplikacji. W ustawieniach pakietu instalacyjnego możesz także utworzyć składniki aplikacji i skonfigurować ustawienia instalacji aplikacji (patrz tabela poniżej). Pakiet instalacyjny zawiera antywirusowe bazy danych z repozytorium Serwera administracyjnego. Możesz [zaktualizować bazy danych w pakiecie instalacyjnym](#), aby zmniejszyć ruch sieciowy podczas aktualizacji baz danych po zainstalowaniu Kaspersky Endpoint Security.

Ustawienia pakietu instalacyjnego

Sekcja	Opis
Składniki ochrony	W tej sekcji możesz wybrać komponenty aplikacji, które będą dostępne. Możesz zmienić zestaw składników aplikacji w późniejszym czasie, korzystając z zadania <i>Zmień składniki aplikacji</i> . Komponent Ochrona przed atakami BadUSB, komponent Endpoint Agent oraz komponenty szyfrowania danych nie są instalowane domyślnie. Te komponenty mogą zostać dodane w ustawieniach pakietu instalacyjnego.
Ustawienia instalacji	<p>Dodaj lokalizację aplikacji do zmiennej środowiskowej %PATH%. Możesz dodać ścieżkę instalacji do zmiennej %PATH% dla wygodnego korzystania z interfejsu wiersza poleceń.</p> <p>Nie chroń procesu instalacji. Ochrona instalacji obejmuje ochronę przed zastąpieniem pakietu dystrybucyjnego szkodliwymi aplikacjami, blokowaniem dostępu do folderu instalacyjnego Kaspersky Endpoint Security, a także blokowaniem dostępu do sekcji rejestru systemu zawierającego klucze aplikacji. Jeżeli aplikacja nie może zostać zainstalowana (na przykład podczas zdalnej instalacji przy użyciu pulpitu zdalnego systemu Windows), zalecane jest wyłączenie ochrony procesu instalacji.</p> <p>Zapewnij kompatybilność z Citrix PVS. Możesz włączyć obsługę Citrix Provisioning Services, aby zainstalować Kaspersky Endpoint Security na maszynie wirtualnej.</p>

Ścieżka folderu instalacyjnego aplikacji. Możesz zmienić ścieżkę instalacji Kaspersky Endpoint Security na komputerze klienckim. Domyślnie, aplikacja jest instalowana w folderze %ProgramFiles%\Kaspersky Lab\Kaspersky Endpoint Security for Windows.

Plik konfiguracyjny. Możesz przesłać plik, który definiuje ustawienia Kaspersky Endpoint Security. Możesz [utworzyć plik konfiguracyjny w interfejsie lokalnym aplikacji](#).

Aktualizowanie baz danych w pakiecie instalacyjnym

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

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

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

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

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Dodatkowe** → **Instalacja zdalna** → **Pakiety instalacyjne**.

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

2. Otwórz właściwości pakietu instalacyjnego.
3. W sekcji **Ogólne** kliknij przycisk **Aktualizuj bazy danych**.

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

[Jak aktualizować antywirusowe bazy danych w pakiecie instalacyjnym za pośrednictwem konsoli Web Console?](#)

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

Spowoduje to otwarcie listy pakietów instalacyjnych pobranych do Web Console.

2. Kliknij nazwę pakietu instalacyjnego Kaspersky Endpoint Security, w którym chcesz zaktualizować antywirusowe bazy danych.

Zostanie otwarte okno właściwości pakietu instalacyjnego.

3. Na zakładce **Informacje ogólne** kliknij odnośnik **Aktualizuj bazy danych**.

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

Tworzenie zadania zdalnej instalacji

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

[Jak utworzyć zadanie zdalnej instalacji w Konsoli administracyjnej \(MMC\)?](#) 

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zadania**.

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Nowe zadanie**.

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

Krok 1. Wybieranie typu zadania

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

Krok 2. Wybieranie pakietu instalacyjnego

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

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

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

Krok 3. Dodatkowe

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

Krok 4. Ustawienia

Skonfiguruj następujące dodatkowe ustawienia aplikacji:

- **Wymuś pobranie pakietu instalacyjnego.** Wybierz metodę instalacji aplikacji:
 - **Przy użyciu Agenta sieciowego.** Jeśli Agent sieciowy nie został zainstalowany na komputerze, w pierwszej kolejności Agent sieciowy zostanie zainstalowany przy użyciu narzędzi systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie zainstalowany przez narzędzia Agenta sieciowego.
 - **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji.** Pakiet instalacyjny jest dostarczany na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji [znajdziesz w pomocy do Kaspersky Security Center](#).
 - **Przy użyciu zasobów systemu operacyjnego przez serwer administracyjny.** Pliki zostaną dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.
- **Zachowanie dla urządzeń zarządzanych przez inne Serwery administracyjne.** Wybierz metodę instalacji Kaspersky Endpoint Security. Jeśli w sieci jest zainstalowanych więcej niż jeden Serwer

administracyjny, te Serwery administracyjne mogą widzieć te same komputery klienckie. Może to spowodować, na przykład, zdalne zainstalowanie aplikacji na tym samym komputerze kilka razy poprzez różne Serwery administracyjne lub inne konflikty.

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

Krok 5. Wybieranie ustawienia ponownego uruchomienia systemu operacyjnego

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

Krok 6. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

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

Krok 7. Wybieranie konta do uruchomienia zadania

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



Krok 8. Konfigurowanie terminarza uruchamiania zadania

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

Krok 9. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład: Zainstaluj Kaspersky Endpoint Security for Windows 11.7.0.

Krok 10. Kończenie tworzenia zadania

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

[Jak utworzyć zadanie zdalnej instalacji w Web Console i Cloud Console?](#) 

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

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

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Security Center**.

2. Na liście rozwijanej **Typ zadania** wybierz **Zdalna instalacja aplikacji**.

3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, Instalacja Kaspersky Endpoint Security dla menadżerów.

4. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

Krok 2. Wybieranie komputerów do instalacji

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

Krok 3. Konfigurowanie pakietu instalacyjnego

W tym kroku skonfiguruj pakiet instalacyjny:

1. Wybierz pakiet instalacyjny Kaspersky Endpoint Security for Windows (11.7.0).

2. Wybierz pakiet instalacyjny Agenta sieciowego.

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

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

- **Przy użyciu Agenta sieciowego.** Jeśli Agent sieciowy nie został zainstalowany na komputerze, w pierwszej kolejności Agent sieciowy zostanie zainstalowany przy użyciu narzędzi systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie zainstalowany przez narzędzia Agenta sieciowego.
- **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji.** Pakiet instalacyjny jest dostarczany na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji [znajdziesz w pomocy do Kaspersky Security Center](#).
- **Przy użyciu zasobów systemu operacyjnego przez serwer administracyjny.** Pliki zostaną dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny.



Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.

4. W polu **Maksymalna liczba jednoczesnych pobierań** ustaw ograniczenie liczby żądań pobrania pakietu instalacyjnego, wysłanych do Serwera administracyjnego. Ograniczenie liczby żądań pomoże w ograniczeniu przeciążenia sieci.
5. W polu **Maksymalna liczba prób instalacji** ustaw ograniczenie liczby prób zainstalowania aplikacji. Jeśli instalacja Kaspersky Endpoint Security zakończy się błędem, zadanie automatycznie uruchomi ponownie instalację.
6. Jeśli to konieczne, odznacz pole **Nie instaluj aplikacji ponownie, jeżeli jest już zainstalowana**. Umożliwi to, na przykład, zainstalowanie jednej z poprzednich wersji aplikacji.
7. Jeśli to konieczne, odznacz pole **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**. Umożliwia to uniknięcie pobrania pakietu dystrybucyjnego aplikacji, jeśli system operacyjny komputera nie spełni wymagań oprogramowania. Jeśli jesteś pewien, że system operacyjny komputera spełnia wymagania oprogramowania, możesz pominąć tę weryfikację.
8. Jeśli to konieczne, zaznacz pole **Przypisz pakiet instalacyjny do zasad grupy Active Directory**. Kaspersky Endpoint Security jest instalowany przy użyciu Agenta sieciowego lub ręcznie przy użyciu Active Directory. Aby zainstalować Agenta sieciowego, zadanie zdalnej instalacji musi być uruchomione z uprawnieniami administratora domeny.
9. Jeśli to konieczne, zaznacz pole **Poproś użytkowników o zamknięcie uruchomionych aplikacji**. Instalacja Kaspersky Endpoint Security zużywa zasoby komputera. Dla wygody użytkownika Kreator instalacji aplikacji wyświetli pytanie o zamknięcie uruchomionych aplikacji przed instalacją. Umożliwi to uniknięcie przerw w działaniu innych aplikacji i zapobiegnie możliwym problemom z komputerem.
10. W sekcji **Zachowanie urządzeń zarządzanych poprzez inne Serwery administracyjne** wybierz metodę instalacji Kaspersky Endpoint Security. Jeśli w sieci jest zainstalowanych więcej niż jeden Serwer administracyjny, te Serwery administracyjne mogą widzieć te same komputery klienckie. Może to spowodować, na przykład, zdalne zainstalowanie aplikacji na tym samym komputerze kilka razy poprzez różne Serwery administracyjne lub inne konflikty.

Krok 4. Wybieranie konta do uruchomienia zadania

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

Krok 5. Kończenie tworzenia zadania

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

Instalowanie aplikacji lokalnie przy użyciu kreatora

Interfejs Kreatora instalacji aplikacji składa się z szeregu okien odpowiadających krokom instalacji aplikacji.

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

1. Skopiuj folder [pakietu dystrybucyjnego](#) na komputer użytkownika.
2. Uruchom setup_ks.exe.

Zostanie uruchomiony Kreator instalacji.

Przygotowanie do instalacji

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

- Obecność zainstalowanego niekompatybilnego oprogramowania (lista niekompatybilnego oprogramowania jest dostępna w pliku incompatible.txt, który znajduje się w [pakiecie dystrybucyjnym](#)).
- [Spełnione są wymagania sprzętowe i programowe](#).
- Użytkownik ma uprawnienia do zainstalowania produktu.

Jeżeli jakiegokolwiek z powyższych wymagań nie jest spełnione, wyświetlony zostanie odpowiedni komunikat.

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

Jeśli wykryte aplikacje obejmują poprzednie wersje Kaspersky Endpoint Security, wszystkie dane, które można przenieść (dane aktywacji i ustawienia aplikacji), zostaną zachowane i użyte podczas instalacji Kaspersky Endpoint Security 11.7.0 for Windows, a poprzednia wersja aplikacji zostanie automatycznie usunięta. Dotyczy to następujących wersji aplikacji:

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (wersja 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (wersja 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (wersja 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (wersja 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (wersja 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 for Windows (wersja 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (wersja 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (wersja 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (wersja 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (wersja 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 for Windows (wersja 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (wersja 11.5.0.590).

- Kaspersky Endpoint Security 11.6.0 for Windows (wersja 11.6.0.394).

Składniki Kaspersky Endpoint Security

Podczas procesu instalacji możesz wybrać składniki Kaspersky Endpoint Security, które zostaną zainstalowane. Komponent Ochrona plików jest obowiązkowym komponentem, który musi zostać zainstalowany. Nie możesz anulować jego instalacji.

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

- [Ochrona przed atakami BadUSB](#).
- [Składniki Szyfrowania danych](#).
- [Składniki Detection and Response](#).

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

Ustawienia zaawansowane

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

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

Dodaj lokalizację aplikacji do zmiennej środowiskowej %PATH%. Możesz dodać ścieżkę instalacji do zmiennej %PATH% dla wygodnego [korzystania z interfejsu wiersza poleceń](#).

Zdalne instalowanie aplikacji przy użyciu System Center Configuration Manager

Te instrukcje dotyczą System Center Configuration Manager 2012 R2.

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

1. Otwórz konsolę Configuration Manager.
2. W prawej części okna, w sekcji **App management** wybierz **Packages**.
3. W górnej części konsoli, w panelu sterowania, kliknij przycisk **Create package**.
Zostanie uruchomiony kreator *New Package and Application Wizard*.
4. W kreatorze New Package and Application Wizard:
 - a. W sekcji **Package**:

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

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

c. W sekcji **Standard program**:

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

d. W sekcji **Requirements**:

- Zaznacz pole **Run another program first**, jeśli przed zainstalowaniem Kaspersky Endpoint Security chcesz uruchomić inną aplikację.
Wybierz aplikację z listy rozwijalnej **Application** lub określ ścieżkę do pliku wykonywalnego tej aplikacji, klikając przycisk **Browse**.
- W sekcji **Platform requirements** zaznacz opcję **This program can run only on specified platforms**, jeśli chcesz, aby aplikacja była instalowana tylko w określonych systemach operacyjnych.
Na poniższej liście zaznacz obok systemów operacyjnych, w których zostanie zainstalowany Kaspersky Endpoint Security.

Ten krok jest opcjonalny.

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

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

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

Zostanie uruchomiony kreator *Deployment Wizard*.

6. W kreatorze *Deployment Wizard*:

a. W sekcji **General**:

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

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

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

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

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

Opis ustawień instalacji pliku setup.ini

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



Plik setup.ini zawiera następujące sekcje:

- `[Setup]` – ustawienia ogólne instalacji aplikacji.
- `[Components]` – wybór instalowanych składników aplikacji. Jeżeli nie określono żadnego składnika, zostaną zainstalowane wszystkie składniki dostępne dla systemu operacyjnego. Ochrona plików jest obowiązkowym komponentem i jest instalowana na komputerze bez względu na ustawienia wskazane w tej sekcji. W tej sekcji nie ma także komponentu Managed Detection and Response. Aby zainstalować ten komponent, musisz [aktywować Managed Detection and Response w Kaspersky Security Center Console](#).
- `[Tasks]` – wybór zadań, które mają zostać włączone do listy zadań Kaspersky Endpoint Security. Jeżeli nie określono żadnego zadania, wszystkie zadania zostają włączone do listy zadań Kaspersky Endpoint Security.

Zamiast wartości 1 możesz użyć wartości `yes`, `on`, `enable` lub `enabled`.

Zamiast wartości 0 możesz użyć wartości `no`, `off`, `disable` lub `disabled`.

Ustawienia pliku setup.ini

Sekcja	Parametr	Opis
<code>[Setup]</code>	<code>InstallDir</code>	Ścieżka do folderu instalacyjnego aplikacji.
	<code>ActivationCode</code>	Kod aktywacyjny Kaspersky Endpoint Security.
	<code>EULA=1</code>	Akceptacja lub odrzucenie warunków Umowy licencyjnej. Umowa licencyjna jest zawarta w pakiecie dystrybucyjnym Kaspersky Endpoint Security . <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">Akceptacja warunków Umowy licencyjnej jest niezbędna do zainstalowania aplikacji lub jej aktualizacji.</div>
	<code>PrivacyPolicy=1</code>	Akceptacja Polityki prywatności. Treść Polityki prywatności znajduje się w pakiecie dystrybucyjnym Kaspersky Endpoint Security .

		<p>Aby zainstalować aplikację lub zaktualizować wersję aplikacji, musisz zaakceptować Politykę prywatności.</p>
	KSN	<p>Akceptacja lub odmowa uczestnictwa w Kaspersky Security Network. Jeśli nie ustawiono wartości dla tego parametru, Kaspersky Endpoint Security wyświetli monit o potwierdzenie zgody lub odmowę uczestniczenia w KSN przy pierwszym uruchomieniu Kaspersky Endpoint Security. Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – zgoda na uczestniczenie w KSN. • 0 – odmowa uczestniczenia w KSN (wartość domyślna). <p>Pakiet dystrybucyjny Kaspersky Endpoint Security jest zoptymalizowany do użycia z Kaspersky Security Network. Jeśli zdecydowałeś się nie uczestniczyć w Kaspersky Security Network, powinieneś zaktualizować Kaspersky Endpoint Security od razu po zakończeniu instalacji.</p>
	Login	<p>Ustaw nazwę użytkownika, aby uzyskać dostęp do funkcji i ustawień Kaspersky Endpoint Security (komponent Ochrona hasłem). Nazwa użytkownika jest ustawiana wraz z parametrami Password i PasswordArea. Nazwa użytkownika KLAdmin jest używana domyślnie.</p>
	Hasło	<p>Określ hasło dostępu do funkcji i ustawień Kaspersky Endpoint Security (hasło jest określane wraz z parametrami Login i PasswordArea).</p> <p>Jeśli określiłeś hasło, ale nie określiłeś nazwy użytkownika z parametrem Login, domyślnie używana będzie nazwa użytkownika KLAdmin.</p>
	PasswordArea	<p>Zakres działania hasła dostępu do funkcji i ustawień Kaspersky Endpoint Security. Jeśli użytkownik spróbuje wykonać działanie, które znajduje się w tym obszarze, Kaspersky Endpoint Security wyświetli monit o podanie danych uwierzytelniających konta użytkownika (parametry Login i Password). Użyj znaku „;” aby określić kilka wartości.</p> <p>Dostępne wartości:</p> <ul style="list-style-type: none"> • SET – modyfikowanie ustawień aplikacji. • EXIT – zakończenie działania aplikacji. • DISPROTECT – wyłączanie komponentów ochrony i zatrzymywanie zadań skanowania. • DISPOLICY – wyłączanie zasady Kaspersky Security Center. • UNINST – usunięcie aplikacji z komputera.

		<ul style="list-style-type: none"> • DISCTRL – wyłączenie składników kontroli. • REMOVELIC – usuwanie klucza. • REPORTS – wyświetlanie raportów.
	SelfProtection	<p>Włączenie lub wyłączenie mechanizmu ochrony instalacji aplikacji. Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – mechanizm ochrony instalacji aplikacji jest włączony (domyślna wartość). • 0 – mechanizm ochrony instalacji aplikacji jest wyłączony. <p>Ochrona instalacji obejmuje ochronę przed zastąpieniem pakietu dystrybucyjnego szkodliwymi aplikacjami, blokowaniem dostępu do folderu instalacyjnego Kaspersky Endpoint Security, a także blokowaniem dostępu do sekcji rejestru systemu zawierającego klucze aplikacji. Jeżeli aplikacja nie może zostać zainstalowana (na przykład podczas zdalnej instalacji przy użyciu pulpitu zdalnego systemu Windows), zalecane jest wyłączenie ochrony procesu instalacji.</p>
	Reboot=1	<p>Automatyczne ponowne uruchamianie komputera, jeśli jest wymagane po zainstalowaniu lub zaktualizowaniu aplikacji. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość, automatyczne ponowne uruchomienie komputera zostanie zablokowane.</p> <p>Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Ponowne uruchomienie jest wymagane tylko wtedy, gdy przed instalacją musisz usunąć niekompatybilne aplikacje. Ponowne uruchomienie może być też wymagane podczas aktualizowania wersji aplikacji.</p>
	AddEnvironment	<p>W zmiennej systemowej %PATH% dodaje ścieżkę dostępu do plików wykonywalnych znajdujących się w folderze instalacyjnym Kaspersky Endpoint Security. Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – do zmiennej %PATH% zostaje dodana ścieżka dostępu do plików wykonywalnych znajdujących się w folderze instalacyjnym Kaspersky Endpoint Security. • 0 – do zmiennej %PATH% nie zostaje dodana ścieżka dostępu do plików wykonywalnych znajdujących się w folderze instalacyjnym Kaspersky Endpoint Security.
	AMPPL	<p>Włącza lub wyłącza ochronę procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL (Antimalware Protected Process Light). Więcej informacji na temat technologii AM-PPL znajdziesz na stronie internetowej firmy Microsoft ²⁴.</p> <p>Technologia AM-PPL jest dostępna dla systemu Windows 10 w wersji 1703 (RS2) lub nowszej oraz systemów operacyjnych Windows Server 2019.</p>

		<p>Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – ochrona procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest włączona. • 0 – ochrona procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest wyłączona.
	SetupReg	<p>Włącza zapisywanie kluczy rejestru z pliku setup.reg do rejestru. Wartość parametru SetupReg: setup.reg.</p>
	EnableTraces	<p>Włączanie lub wyłączanie śledzenia aplikacji. Po uruchomieniu, program Kaspersky Endpoint Security zapisuje pliki śledzenia w folderze %ProgramData%\Kaspersky Lab\KES\Traces. Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – śledzenie jest włączone. • 0 – śledzenie jest wyłączone (wartość domyślna).
	TracesLevel	<p>Poziom szczegółowości śledzenia. Dostępne wartości:</p> <ul style="list-style-type: none"> • 100 (krytyczny). Tylko wiadomości dotyczące błędów krytycznych. • 200 (wysoki). Wiadomości o wszystkich błędach, w tym błędach krytycznych. • 300 (diagnostyczny). Wiadomości o wszystkich błędach, a także ostrzeżenia. • 400 (ważny). Wszystkie wiadomości o błędach, ostrzeżenia i dodatkowe informacje. • 500 (normalny). Wiadomości o wszystkich błędach i ostrzeżeniach, a także szczegółowe informacje o działaniu aplikacji w trybie normalnym (domyślnie). • 600 (niski). Wszystkie wiadomości.
	RESTAPI	<p>Zarządzanie aplikacją za pośrednictwem interfejsu API REST. Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, należy podać nazwę użytkownika (parametr RESTAPI_User).</p> <p>Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – zarządzanie za pośrednictwem interfejsu API REST jest dozwolone. • 0 – zarządzanie za pośrednictwem interfejsu API REST jest zablokowane (wartość domyślna).

		Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, zarządzanie przy użyciu systemów administracyjnych musi być dozwolone. W tym celu ustaw parametr AdminKitConnector=1. Jeśli zarządzasz aplikacją za pośrednictwem interfejsu API REST, zarządzanie aplikacją przy użyciu systemów administracyjnych firmy Kaspersky jest niemożliwe.
	RESTAPI_User	Nazwa użytkownika konta domeny Windows używanego do zarządzania aplikacją za pośrednictwem interfejsu API REST. Zarządzanie aplikacją za pośrednictwem interfejsu API REST jest dostępne tylko dla tego użytkownika. Wpisz nazwę użytkownika w formacie <DOMAIN>\<UserName> (na przykład: RESTAPI_User=COMPANY\Administrator). Możesz wybrać tylko jednego użytkownika do pracy z interfejsem API REST. Dodanie nazwy użytkownika jest wymaganiem wstępnym zarządzania aplikacją za pośrednictwem interfejsu API REST.
	RESTAPI_Port	Port używany do zarządzania aplikacją za pośrednictwem interfejsu API REST. Domyślnie używany jest port 6782.
	RESTAPI_Certificate	Certyfikat do identyfikowania żądań (na przykład, RESTAPI_Certificate=C:\cert.pem). Bezpieczna interakcja Kaspersky Endpoint Security z klientem REST wymaga skonfigurowania identyfikacji żądania. W tym celu należy zainstalować certyfikat i podpisać ładunek każdego żądania.
[Components]	ALL	Instalacja wszystkich komponentów. Jeśli dla parametru określono wartość 1, zostaną zainstalowane wszystkie komponenty, niezależnie od ustawień instalacji pojedynczych składników. Ze względu na nowe sposoby obsługi rozwiązań Detection and Response, na komputerze są instalowane komponenty Endpoint Detection and Response Optimum oraz Kaspersky Sandbox. Komponent Endpoint Agent nie jest konfigurowany z tą konfiguracją aplikacji.
	MailThreatProtection	Ochrona poczty.
	WebThreatProtection	Ochrona WWW.
	AMSI	Ochrona AMSI.
	HostIntrusionPrevention	Ochrona przed włamaniami.
	BehaviorDetection	Wykrywanie zachowania.
	ExploitPrevention	Ochrona przed exploitami.
	RemediationEngine	Silnik korygujący.
	Zapora sieciowa	Zapora sieciowa.
		Ochrona sieci.

	NetworkThreatProtection	
	WebControl	Kontrola sieci.
	DeviceControl	Kontrola urządzeń.
	ApplicationControl	Kontrola aplikacji.
	AdaptiveAnomaliesControl	Adaptacyjna kontrola anomalii.
	FileEncryption	Biblioteki Szyfrowania na poziomie plików.
	DiskEncryption	Biblioteki Szyfrowania całego dysku.
	BadUSBAttackPrevention	Ochrona przed atakami BadUSB.
	AntiAPT	<p>Endpoint Agent. Endpoint Agent instaluje Kaspersky Endpoint Agent w celu ułatwienia interakcji aplikacji i rozwiązań Kaspersky do wykrywania zaawansowanych zagrożeń (na przykład, Kaspersky Sandbox).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Komponent jest niekompatybilny z komponentami Endpoint Detection and Response Optimum (EDR) oraz Kaspersky Sandbox (SB).</p> </div>
	EDR	<p>Endpoint Detection and Response Optimum (EDR Optimum).</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Komponent jest niekompatybilny z komponentem Endpoint Agent (AntiAPT).</p> </div>
	SB	<p>Kaspersky Sandbox.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Komponent jest niekompatybilny z komponentem Endpoint Agent (AntiAPT).</p> </div>
	AdminKitConnector	<p>Zarządzanie aplikacjami za pomocą systemów administracyjnych. Systemy administracyjne obejmują, na przykład, Kaspersky Security Center. Oprócz systemów administracyjnych Kaspersky możesz korzystać z rozwiązań innych firm. Kaspersky Endpoint Security oferuje w tym celu interfejs API.</p> <p>Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – dozwolone jest zarządzanie aplikacjami za pomocą systemów administracyjnych (wartość domyślna). • 0 – zarządzanie aplikacjami jest dozwolone tylko przez interfejs lokalny.
[Zadania]	ScanMyComputer	Zadanie Pełnego skanowania. Dostępne wartości:

		<ul style="list-style-type: none"> • 1 – zadanie zostaje włączone do listy zadań Kaspersky Endpoint Security. • 0 – zadanie nie zostaje włączone do listy zadań Kaspersky Endpoint Security.
	ScanCritical	<p>Zadanie Skanowanie obszarów krytycznych. Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – zadanie zostaje włączone do listy zadań Kaspersky Endpoint Security. • 0 – zadanie nie zostaje włączone do listy zadań Kaspersky Endpoint Security.
	Updater	<p>Zadanie aktualizacji. Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – zadanie zostaje włączone do listy zadań Kaspersky Endpoint Security. • 0 – zadanie nie zostaje włączone do listy zadań Kaspersky Endpoint Security.

Zmiana składników aplikacji

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

- Lokalnie, za pomocą Kreatora instalacji.

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

- Zdalnie, przy użyciu Kaspersky Security Center.

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

Zmieniając komponenty aplikacji, należy mieć na uwadze następujące kwestie:

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

[Jak dodawać lub usuwać komponenty aplikacji w Konsoli administracyjnej \(MMC\)?](#)

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zadania**.

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Nowe zadanie**.

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

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (11.7.0)** → **Zmiana składników aplikacji**.

Krok 2. Ustawienia zadania zmiany składników aplikacji

Wybierz składniki aplikacji, które będą dostępne na komputerze użytkownika.

Zaznacz pole **Usuń niekompatybilne aplikacje firm trzecich**. Listę niekompatybilnych aplikacji można przejrzeć w pliku `incompatible.txt`, który znajduje się w [pakiecie dystrybucyjnym](#). Jeśli na komputerze są zainstalowane niekompatybilne aplikacje, instalacja Kaspersky Endpoint Security zakończy się błędem.

Jeśli to konieczne, włącz [ochronę hasłem](#) dla działania zadania:

1. Kliknij przycisk **Dodatkowe**.

2. Zaznacz pole **Użyj hasła do modyfikacji zestawu składników aplikacji**.

3. Wprowadź dane uwierzytelniające konta użytkownika KLAdmin.

Krok 3. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

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

Krok 4. Konfigurowanie terminarza uruchamiania zadania

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

Krok 5. Definiowanie nazwy zadania

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

Krok 6. Kończenie tworzenia zadania

Zakończ działanie Kreatora. W razie potrzeby zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

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

[Jak dodawać lub usuwać składniki aplikacji w Web Console i Cloud Console?](#) 

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

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

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.
2. Na liście rozwijanej **Typ zadania** wybierz **Zmiana składników aplikacji**.
3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, **Dodaj komponent Kontrola aplikacji**.
4. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

Krok 2. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

Krok 3. Kończenie tworzenia zadania

Zaznacz pole **Otwórz szczegóły zadania po jego utworzeniu** i zakończ działanie Kreatora. We właściwościach zadania wybierz zakładkę **Ustawienia aplikacji** i wybierz składniki aplikacji, które będą dostępne.

Jeśli to konieczne, włącz [ochronę hasłem](#) dla działania zadania:

1. W sekcji **Ustawienia zaawansowane** zaznacz pole **Użyj hasła do modyfikacji zestawu składników aplikacji**.
2. Wprowadź dane uwierzytelniające konta użytkownika KLAdmin.

Zapisz zmiany i uruchom zadanie.

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

Aktualizowanie z poprzedniej wersji aplikacji

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

- Przed rozpoczęciem aktualizacji zalecamy zamknięcie wszystkich aktywnych aplikacji.

- Jeśli komputer ma dyski twarde, które są zaszyfrowane przy użyciu [Szyfrowania całego dysku \(FDE\)](#), musisz odszyfrować wszystkie zaszyfrowane dyski twarde, aby zaktualizować Kaspersky Endpoint Security z wersji 10 do wersji 11.0.0 lub nowszej.

Przed aktualizacją Kaspersky Endpoint Security blokuje funkcjonalność Szyfrowanie całego dysku. Jeśli nie można odblokować Szyfrowania całego dysku, instalacja aktualizacji nie zostanie uruchomiona. Po zaktualizowaniu aplikacji przywrócona zostanie funkcjonalność Szyfrowanie całego dysku.

Kaspersky Endpoint Security obsługuje aktualizacje następujących wersji aplikacji:

- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (wersja 10.3.3.275).
- Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 4 for Windows (wersja 10.3.3.304).
- Kaspersky Endpoint Security 11.0.0 for Windows (wersja 11.0.0.6499).
- Kaspersky Endpoint Security 11.0.1 for Windows (wersja 11.0.1.90).
- Kaspersky Endpoint Security 11.0.1 for Windows SF1 (wersja 11.0.1.90).
- Kaspersky Endpoint Security 11.1.0 for Windows (wersja 11.1.0.15919).
- Kaspersky Endpoint Security 11.1.1 for Windows (wersja 11.1.1.126).
- Kaspersky Endpoint Security 11.2.0 for Windows (wersja 11.2.0.2254).
- Kaspersky Endpoint Security 11.2.0 for Windows CF1 (wersja 11.2.0.2254).
- Kaspersky Endpoint Security 11.3.0 for Windows (wersja 11.3.0.773).
- Kaspersky Endpoint Security 11.4.0 for Windows (wersja 11.4.0.233).
- Kaspersky Endpoint Security 11.5.0 for Windows (wersja 11.5.0.590).
- Kaspersky Endpoint Security 11.6.0 for Windows (wersja 11.6.0.394).

Podczas aktualizacji Kaspersky Endpoint Security 10 Service Pack 2 for Windows do Kaspersky Endpoint Security 11.7.0 for Windows, pliki, które w poprzedniej wersji aplikacji zostały umieszczone w Kopii zapasowej lub Kwarantannie, zostaną przeniesione do Kopii zapasowej w nowej wersji aplikacji. W przypadku wersji wcześniejszych niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, pliki, które w poprzedniej wersji zostały umieszczone w Kopii zapasowej i Kwarantannie, nie zostaną przeniesione do nowszej wersji.

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

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

- zdalnie, za pomocą [programu System Center Configuration Manager](#).

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

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

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

- Serwer administracyjny Kaspersky Security Center.

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

Deinstalacja aplikacji

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

Program Kaspersky Endpoint Security można usunąć z komputera na następujące sposoby:

- lokalnie, za pomocą [Kreatora instalacji](#);
- lokalnie, z poziomu [wiersza poleceń](#);
- zdalnie, przy użyciu Kaspersky Security Center (więcej informacji znajdziesz w [systemie pomocy programu Kaspersky Security Center](#));
- zdalnie, za pośrednictwem Edytora zarządzania zasadami grupy Microsoft Windows (więcej informacji można znaleźć na [stronie pomocy technicznej firmy Microsoft](#)).

Jeśli podczas instalacji wybrałeś komponent Endpoint Agent, na komputerze zostaną zainstalowane dwie następujące aplikacje: Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Po odinstalowaniu Kaspersky Endpoint Security, Kaspersky Endpoint Agent również zostanie odinstalowany automatycznie.

Deinstalacja za pośrednictwem Kaspersky Security Center

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

[Jak usunąć aplikację za pomocą Konsoli administracyjnej \(MMC\)?](#)

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zadania**.

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Nowe zadanie**.

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

Krok 1. Wybieranie typu zadania

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

Krok 2. Wybieranie aplikacji do usunięcia

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

Krok 3. Ustawienia zadania do odinstalowania aplikacji

Wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

Krok 4. Ustawienia narzędzia deinstalacyjnego

Skonfiguruj następujące dodatkowe ustawienia aplikacji:

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

Jeśli operacja dezinstalacji aplikacji jest [chroniona hasłem](#), wykonaj następujące czynności:

1. Zaznacz pole **Użyj hasła deinstalacyjnego**.

2. Kliknij przycisk **Edytuj**.

3. Wpisz hasło do konta KLAdmin.

Krok 5. Wybieranie ustawienia ponownego uruchomienia systemu operacyjnego

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

Krok 6. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

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

Krok 7. Wybieranie konta do uruchomienia zadania

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

Krok 8. Konfigurowanie terminarza uruchamiania zadania

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

Krok 9. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład: `Usuń Kaspersky Endpoint Security 11.7.0`.

Krok 10. Kończenie tworzenia zadania

Zakończ działanie Kreatora. W razie potrzeby zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

Aplikacja zostanie odinstalowana w trybie cichym.

[Jak usunąć aplikację za pomocą Web Console i Cloud Console?](#) 

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

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

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Security Center**.

2. Na liście rozwijanej **Typ zadania** wybierz **Zdalna dezinstalacja aplikacji**.

3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, **Usuń Kaspersky Endpoint Security z komputerów pomocy technicznej**.

4. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

Krok 2. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

Krok 3. Konfigurowanie ustawień dezinstalacji aplikacji

W tym kroku skonfiguruj ustawienia dezinstalacji aplikacji:

1. Wybierz **Odinstaluj zarządzaną aplikację**.

2. Wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

3. **Wymuś pobranie narzędzia dezinstalacyjnego**. Wybierz metodę dostarczenia narzędzia:

- **Przy użyciu Agenta sieciowego**. Jeśli Agent sieciowy nie został zainstalowany na komputerze, w pierwszej kolejności Agent sieciowy zostanie zainstalowany przy użyciu narzędzi systemu operacyjnego. Następnie Kaspersky Endpoint Security zostanie odinstalowany przez narzędzia Agenta sieciowego.
- **Przy użyciu zasobów systemu operacyjnego przez serwer administracyjny**. Narzędzie zostanie dostarczone na komputery klienckie przy użyciu zasobów systemu operacyjnego przez Serwer administracyjny. Możesz wybrać tę opcję, jeśli na komputerze klienckim nie ma zainstalowanego Agenta sieciowego, ale komputer kliencki jest w tej samej sieci co Serwer administracyjny.
- **Przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji**. Narzędzie jest dostarczane na komputery klienckie przy użyciu zasobów systemu operacyjnego poprzez punkty dystrybucji. Możesz wybrać tę opcję, jeżeli w sieci jest przynajmniej jeden punkt dystrybucyjny. Więcej informacji o punktach dystrybucji znajdziesz w [pomocy do Kaspersky Security Center](#).

4. W polu **Maksymalna liczba jednoczesnych pobierań** ustaw limit liczby żądań wysłanych do Serwera administracyjnego w celu pobrania narzędzia do odinstalowania aplikacji. Ograniczenie liczby żądań pomoże

w ograniczeniu przeciążenia sieci.

5. W polu **Maksymalna liczba prób dezinstalacji** ustaw ograniczenie liczby prób odinstalowania aplikacji. Jeśli dezinstalacja Kaspersky Endpoint Security zakończy się błędem, zadanie automatycznie uruchomi ponownie dezinstalację.
6. Jeśli to konieczne, odznacz pole **Zweryfikuj rodzaj systemu operacyjnego przed pobraniem**. Umożliwia to uniknięcie pobrania narzędzia do dezinstalacji, jeśli system operacyjny komputera nie spełni wymagań oprogramowania. Jeśli jesteś pewien, że system operacyjny komputera spełnia wymagania oprogramowania, możesz pominąć tę weryfikację.

Krok 4. Wybieranie konta do uruchomienia zadania

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

Krok 5. Kończenie tworzenia zadania

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

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

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

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

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Kliknij zadanie **Zdalna dezinstalacja aplikacji** z programu Kaspersky Security Center.
Zostanie otwarte okno właściwości zadania.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Zaznacz pole **Użyj hasła dezinstalacyjnego**.
5. Wpisz hasło do konta KLAdmin.
6. Kliknij przycisk **Zapisz**.

Dezinstalowanie aplikacji przy użyciu Kreatora

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

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

Możesz zapisać następujące dane:

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

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

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

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

Licencjonowanie aplikacji

Ta sekcja zawiera informacje o ogólnych pojęciach związanych z licencjonowaniem aplikacji.

Informacje o Umowie licencyjnej

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

Przed rozpoczęciem korzystania z aplikacji należy dokładnie przeczytać Umowę licencyjną.

Warunki Umowy licencyjnej możesz sprawdzić:

- Podczas [instalowania Kaspersky Endpoint Security w trybie interaktywnym](#).
- W pliku license.txt. Ten dokument znajduje się w [pakiecie dystrybucyjnym aplikacji](#) i znajduje się również w folderze instalacyjnym aplikacji %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Endpoint Security for Windows\Doc\

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

Informacje o licencji

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

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

Dostępne są następujące typy licencji:

- *Testowa* – jest to darmowa licencja udostępniana w celu zapoznania użytkowników z programem.
Licencja testowa ma zazwyczaj krótki okres ważności. Po wygaśnięciu licencji testowej wszystkie funkcje programu Kaspersky Endpoint Security stają się niedostępne. Aby kontynuować korzystanie z aplikacji, musisz zakupić licencję komercyjną.
Możesz aktywować aplikację przy użyciu licencji testowej tylko raz.
- *Komercyjna* – płatna licencja oferowana podczas zakupu Kaspersky Endpoint Security.
Funkcjonalność aplikacji, objęta licencją komercyjną, zależy od wyboru produktu. Wybrany produkt jest wyszczególniony w [certyfikacie licencji](#). Informacje o dostępnych produktach można znaleźć na [stronie internetowej firmy Kaspersky](#).
Po wygaśnięciu licencji komercyjnej zostaną włączone kluczowe funkcje aplikacji. Aby kontynuować korzystanie z aplikacji, musisz odnowić licencję komercyjną. Jeśli nie planujesz odnowienia licencji, musisz usunąć aplikację z komputera.

Informacje o certyfikacie licencji

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

Certyfikat licencji zawiera następujące informacje o licencji:

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

Informacje o subskrypcji

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

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

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

Aby używać Kaspersky Endpoint Security z subskrypcją, należy użyć [kodu aktywacyjnego](#), otrzymanego od dostawcy usługi. Po zastosowaniu kodu aktywacyjnego zostanie zainstalowany aktywny klucz. Aktywny klucz określa licencję do używania aplikacji z subskrypcją. Nie można dodać zapasowego klucza w ramach subskrypcji.

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

Informacje o kluczu licencyjnym

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

[Certyfikat licencyjny](#) nie jest udostępniany dla kluczy dodawanych z opcją subskrypcji.

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

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

Istnieją dwa typy kluczy: aktywny i zapasowy.

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

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

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

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

Informacje o kodzie aktywacyjnym

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

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

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

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

Informacje o pliku klucza

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

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

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

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

W celu odzyskania pliku klucza:

- Skontaktuj się ze sprzedawcą licencji.
- Uzyskaj plik klucza na [stronie internetowej Kaspersky](#) w oparciu o istniejący kod aktywacyjny.

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

Aktywowanie aplikacji

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

Możesz aktywować aplikację na jeden z następujących sposobów:

- Lokalnie, z poziomu interfejsu aplikacji, używając [Kreatora aktywacji](#). W ten sposób możesz dodać aktywny i zapasowy klucz.
- Zdalnie, przy użyciu [pakietu programu Kaspersky Security Center](#), tworząc i uruchamiając zadanie dodania klucza licencyjnego. W ten sposób możesz dodać aktywny i zapasowy klucz.
- Zdalnie, poprzez dystrybucję plików kluczy i kodów aktywacyjnych przechowywanych w pamięci kluczy Serwera administracyjnego Kaspersky Security Center na komputery klienckie. Bardziej szczegółowe informacje na temat dystrybucji kluczy *można znaleźć* w [systemie pomocy programu Kaspersky Security Center](#). W ten sposób możesz dodać aktywny i zapasowy klucz.

W pierwszej kolejności rozsyłane są kody aktywacyjne z opcją subskrypcji.

- Korzystając z [wiersza poleceń](#).

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

Aktywowanie aplikacji za pośrednictwem Kaspersky Security Center

Możesz aktywować aplikację zdalnie za pośrednictwem Kaspersky Security Center na następujące sposoby:

- Przy pomocy zadania *Dodaj klucz*.

Ta metoda umożliwi dodanie klucza do określonego komputera lub do komputerów, które są częścią grupy administracyjnej.


- Rozsyłając klucz, który jest przechowywany na Serwerze administracyjnym Kaspersky Security Center, na komputery.

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

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

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

Możesz monitorować użycie licencji na następujące sposoby:

- Przejrzyj *Raport użycia klucza* dla infrastruktury organizacji (**Monitorowanie i raportowanie** → **Raporty**).
- Przejrzyj stany komputerów na zakładce **Urządzenia** → **Zarządzane urządzenia**. Jeśli aplikacja nie została aktywowana, komputer będzie miał stan  oraz opis stanu **Aplikacja nie została aktywowana**.
- Przejrzyj informacje o licencji we właściwościach komputera.
- Przejrzyj właściwości klucza (**Działania** → **Licencjonowanie**).

[Jak aktywować aplikację w Konsoli administracyjnej \(MMC\)?](#)

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zadania**.

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Nowe zadanie**.

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

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (11.7.0)** → **Dodaj klucz**.

Krok 2. Dodawanie klucza

Wprowadź [kod aktywacyjny](#) lub wybierz plik klucza.

Więcej informacji na temat dodawania kluczy do repozytorium Kaspersky Security Center *można znaleźć w [pomocy do Kaspersky Security Center](#)*.

Krok 3. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

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

Krok 4. Konfigurowanie terminarza uruchamiania zadania

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

Krok 5. Definiowanie nazwy zadania

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

Krok 6. Kończenie tworzenia zadania

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

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

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

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

2. Na liście rozwijanej **Typ zadania** wybierz **Dodaj klucz**.

3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, Aktywacja Kaspersky Endpoint Security for Windows.

4. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania. Kliknij przycisk **Dalej**.

Krok 2. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

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

Krok 3. Wybieranie licencji

Wybierz licencję, której chcesz użyć do aktywacji aplikacji. Kliknij przycisk **Dalej**.

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

Krok 4. Kończenie tworzenia zadania

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

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

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

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Licencje Kaspersky**.
Zostanie otwarta lista kluczy licencyjnych.
2. Otwórz właściwości klucza licencyjnego.
3. W sekcji **Ogólne** zaznacz pole **Klucz licencyjny rozesłany automatycznie**.
4. Zapisz swoje zmiany.

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

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

1. W oknie głównym Web Console wybierz **Operacje** → **Licencjonowanie** → **Licencje Kaspersky**.
Zostanie otwarta lista kluczy licencyjnych.
2. Otwórz właściwości klucza licencyjnego.
3. Na zakładce **Ogólne** przełącz przycisk przełącznika **Roześlij klucz licencyjny automatycznie**.
4. Zapisz swoje zmiany.

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

Aktywacja aplikacji za pomocą Kreatora aktywacji

W celu aktywacji programu Kaspersky Endpoint Security przy użyciu Kreatora aktywacji:

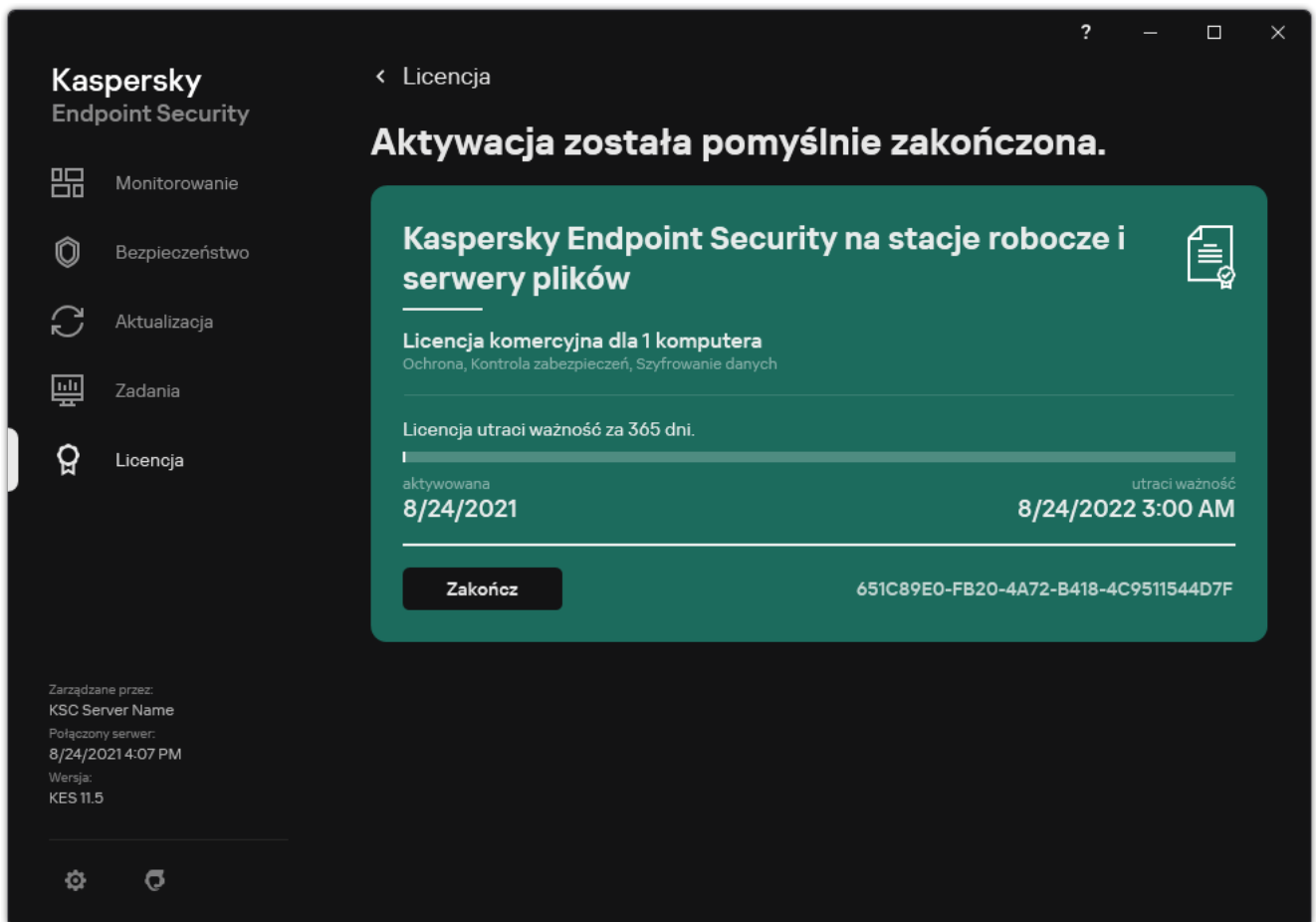
1. W oknie głównym aplikacji przejdź do sekcji **Licencja**.
2. Kliknij **Aktywuj aplikację przy użyciu nowej licencji**.

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

Przeglądanie informacji o licencji

W celu przejrzania informacji o licencji:

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



Okno Licencjonowanie

Sekcja wyświetla następujące szczegóły:

- **Stan klucza.** Na komputerze może być przechowywanych kilka [kluczy](#). Istnieją dwa typy kluczy: aktywny i zapasowy. Aplikacja może posiadać tylko jeden aktywny klucz. Klucz zapasowy może stać się aktywny tylko wtedy, gdy aktywny klucz utraci ważność lub jeśli aktywny klucz został usunięty przy pomocy przycisku **Usuń**.
- **Nazwa aplikacji.** Pełna nazwa zakupionej aplikacji firmy Kaspersky.
- **Licencja.** Dostępne są następujące [typy licencji](#): testowa i komercyjna.
- **Funkcjonalność.** Funkcje aplikacji dostępne w posiadanej licencji. Funkcje mogą obejmować Ochronę, Kontrolę zabezpieczeń, Szyfrowanie danych i inne. Lista dostępnych funkcji znajduje się również w Certyfikacie licencji.
- **Dodatkowe informacje o licencji.** Data początkowa i data końcowa okresu ważności licencji (tylko dla klucza aktywnego), pozostały czas trwania okresu ważności.

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

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

W oknie Licencjonowanie wykonaj jedną z następujących czynności:

- **Kup licencję / Odnów licencję.** Otwiera stronę sklepu internetowego Kaspersky, w którym możesz zakupić lub odnowić licencję. W tym celu wprowadź informacje o swojej firmie i zapłać za zamówienie.
- **Aktywuj aplikację przy użyciu nowej licencji.** Zostanie uruchomiony Kreator aktywacji aplikacji. W tym kreatorze możesz dodać klucz, korzystając z kodu aktywacyjnego lub pliku klucza. Kreator aktywacji aplikacji umożliwia dodanie aktywnego klucza i tylko jednego klucza zapasowego.

Kupowanie licencji

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

W celu zakupu licencji:

1. W oknie głównym aplikacji przejdź do sekcji **Licencja**.
2. Wykonaj jedną z poniższych czynności:
 - Jeśli nie dodano żadnego klucza lub dodano klucz dla licencji testowej, kliknij przycisk **Kup licencję**.
 - Jeżeli dodano klucz dla licencji komercyjnej, kliknij przycisk **Odnów licencję**.

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

Odnawianie subskrypcji

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

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

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

Możesz odnowić subskrypcję na stronie internetowej dostawcy usługi.

W celu odwiedzenia strony dostawcy usługi z poziomu interfejsu aplikacji:

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

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

Przekazywanie danych

Przekazywanie danych zgodnie z Umową licencyjną

Jeśli do aktywacji Kaspersky Endpoint Security zostanie użyty [kod aktywacyjny](#), użytkownik zgadza się okresowo automatycznie wysyłać do Kaspersky następujące informacje w celu weryfikacji prawidłowego korzystania z aplikacji:

- Typ, wersję i lokalizację Kaspersky Endpoint Security;
- Wersje zainstalowanych aktualizacji dla Kaspersky Endpoint Security;
- Identyfikator komputera i identyfikator konkretnej instalacji Kaspersky Endpoint Security na komputerze;
- Numer seryjny i identyfikator aktywnego klucza;
- Typ, wersję i szybkość transmisji bitów systemu operacyjnego oraz nazwę środowiska wirtualnego (jeśli Kaspersky Endpoint Security jest zainstalowany w środowisku wirtualnym);
- Identyfikatory składników Kaspersky Endpoint Security, które są aktywne podczas przesyłania informacji.

Kaspersky może również wykorzystywać te informacje do generowania statystyk dotyczących rozpowszechniania i użytkowania oprogramowania Kaspersky.

Korzystając z kodu aktywacyjnego, zgadzasz się na automatyczne przesyłanie danych wymienionych powyżej. Jeśli nie zgadzasz się na przesłanie tych informacji do Kaspersky, powinieneś użyć [pliku klucza](#) do aktywacji Kaspersky Endpoint Security.

Akceptując warunki Umowy licencyjnej, wyrażasz zgodę na automatyczne przesyłanie następujących informacji:

- Podczas aktualizacji wersji Kaspersky Endpoint Security:
 - Wersji Kaspersky Endpoint Security;
 - ID programu Kaspersky Endpoint Security;
 - Aktywnego klucza;
 - Unikatowego numeru ID uruchomienia zadania aktualizacji;
 - Unikatowego numeru ID instalacji Kaspersky Endpoint Security.
- Podczas klikania następujących odnośników w interfejsie Kaspersky Endpoint Security:
 - Wersji Kaspersky Endpoint Security;
 - Wersji systemu operacyjnego;
 - Daty aktywacji Kaspersky Endpoint Security;
 - Daty wygaśnięcia licencji;
 - Daty utworzenia klucza;

- Daty instalacji Kaspersky Endpoint Security;
- ID programu Kaspersky Endpoint Security;
- ID wykrytej luki w systemie operacyjnym;
- ID ostatniej aktualizacji zainstalowanej dla Kaspersky Endpoint Security;
- Sumy kontrolnej wykrytego pliku z zagrożeniem oraz nazwy tego zagrożenia zgodnej z klasyfikacją Kaspersky;
- Kategorii błędu aktywacji Kaspersky Endpoint Security;
- Kodu błędu aktywacji Kaspersky Endpoint Security;
- Liczby dni pozostałych do wygaśnięcia klucza;
- Liczby dni, jaka minęła od dodania klucza;
- Liczby dni, jaka minęła od wygaśnięcia licencji;
- Liczby komputerów, na których zastosowana jest aktywna licencja;
- Aktywnego klucza;
- Okresu ważności licencji Kaspersky Endpoint Security;
- Bieżącego stanu licencji;
- Typu aktywnej licencji;
- Typu aplikacji;
- Unikatowego numeru ID uruchomienia zadania aktualizacji;
- Unikatowego numeru ID instalacji Kaspersky Endpoint Security na komputerze;
- Języka interfejsu Kaspersky Endpoint Security.

Kaspersky chroni otrzymywane informacje zgodnie z wymogami wynikającymi z przepisów prawa oraz zasadami obowiązującymi w Kaspersky. Dane są przesyłane za pośrednictwem zaszyfrowanych kanałów komunikacji.

Przeczytaj Umowę licencyjną i odwiedź [stronę internetową Kaspersky](#), aby dowiedzieć się więcej o otrzymywaniu, przetwarzaniu, przechowywaniu i niszczeniu przez Kaspersky informacji dotyczących korzystania z aplikacji po zaakceptowaniu Umowy licencyjnej i Oświadczenia Kaspersky Security Network. Pliki license.txt i ksn_<ID języka>.txt zawierają treść Umowy licencyjnej i Oświadczenia Kaspersky Security Network i można je znaleźć w [pakiecie dystrybucyjnym](#) aplikacji.

Przekazywanie danych podczas korzystania z Kaspersky Security Network

Zestaw danych, jaki Kaspersky Endpoint Security wysyła do Kaspersky, zależy od typu licencji i ustawień korzystania z Kaspersky Security Network.

Korzystanie z KSN zgodnie z licencją na więcej niż 4 komputerach

Akceptując Oświadczenie Kaspersky Security Network, wyrażasz zgodę na automatyczne przesyłanie następujących informacji:

- informacje o aktualizacjach konfiguracji KSN: identyfikator aktywnej konfiguracji, identyfikator otrzymanej konfiguracji, kod błędu dla aktualizacji konfiguracji;
- informacje o plikach i adresach URL wymagających skanowania: sumy kontrolne skanowanych plików (MD5, SHA2-256, SHA1) i wzorce plików (MD5), rozmiar wzorca, typ wykrytego zagrożenia i jego nazwę według klasyfikacji Posiadacza Praw, identyfikator dla antywirusowych baz danych, adres URL, którego reputacja jest sprawdzana, a także adres URL strony odsyłającej, identyfikator protokołu połączenia oraz numer używanego portu;
- ID zadania skanowania, które wykryło zagrożenie;
- informacje o używanych certyfikatach cyfrowych, wymagane do zweryfikowania ich autentyczności: sumy kontrolne (SHA256) certyfikatu użytego do podpisania przeskanowanego obiektu oraz klucz publiczny certyfikatu;
- identyfikator komponentu Oprogramowania przeprowadzającego skanowanie;
- identyfikatory antywirusowych baz danych i zapisów w tych antywirusowych bazach danych;
- informacje o aktywności Oprogramowania na Komputerze: podpisany nagłówek biletu z usługi aktywacji (identyfikator regionalnego centrum aktywacji, suma kontrolna kodu aktywacyjnego, suma kontrolna biletu, data utworzenia biletu, unikatowy identyfikator biletu, wersja biletu, stan licencji, data i godzina rozpoczęcia/zakończenia okresu ważności biletu, unikatowy identyfikator licencji, wersja licencji), identyfikator certyfikatu, użytego do podpisania nagłówka biletu, suma kontrolna (MD5) pliku klucza;
- informacje o Oprogramowaniu Posiadacza praw: pełna wersja, typ, wersja protokołu użytego do nawiązania połączenia z usługami Kaspersky.

Korzystanie z KSN zgodnie z licencją na 5 lub więcej komputerach

Akceptując Oświadczenie Kaspersky Security Network, wyrażasz zgodę na automatyczne przesyłanie następujących informacji:

Jeśli pole **Kaspersky Security Network** jest zaznaczone, a pole **Włącz rozszerzony tryb KSN** jest odznaczone, aplikacja przesyła następujące informacje:

- informacje o aktualizacjach konfiguracji KSN: identyfikator aktywnej konfiguracji, identyfikator otrzymanej konfiguracji, kod błędu dla aktualizacji konfiguracji;
- informacje o plikach i adresach URL wymagających skanowania: sumy kontrolne skanowanych plików (MD5, SHA2-256, SHA1) i wzorce plików (MD5), rozmiar wzorca, typ wykrytego zagrożenia i jego nazwę według klasyfikacji Posiadacza Praw, identyfikator dla antywirusowych baz danych, adres URL, którego reputacja jest sprawdzana, a także adres URL strony odsyłającej, identyfikator protokołu połączenia oraz numer używanego portu;
- ID zadania skanowania, które wykryło zagrożenie;
- informacje o używanych certyfikatach cyfrowych, wymagane do zweryfikowania ich autentyczności: sumy kontrolne (SHA256) certyfikatu użytego do podpisania przeskanowanego obiektu oraz klucz publiczny certyfikatu;
- identyfikator komponentu Oprogramowania przeprowadzającego skanowanie;

- identyfikatory antywirusowych baz danych i zapisów w tych antywirusowych bazach danych;
- informacje o aktywności Oprogramowania na Komputerze: podpisany nagłówek biletu z usługi aktywacji (identyfikator regionalnego centrum aktywacji, suma kontrolna kodu aktywacyjnego, suma kontrolna biletu, data utworzenia biletu, unikatowy identyfikator biletu, wersja biletu, stan licencji, data i godzina rozpoczęcia/zakończenia okresu ważności biletu, unikatowy identyfikator licencji, wersja licencji), identyfikator certyfikatu, użytego do podpisania nagłówka biletu, suma kontrolna (MD5) pliku klucza;
- informacje o Oprogramowaniu Posiadacza praw: pełna wersja, typ, wersja protokołu użytego do nawiązania połączenia z usługami Kaspersky.

Jeśli pole **Włącz rozszerzony tryb KSN** jest zaznaczone wraz z polem **Kaspersky Security Network**, oprócz powyższych informacji aplikacja przesyła także następujące informacje:

- informacje o wynikach kategoryzacji żądanych zasobów internetowych, które zawierają przetwarzane adresy URL i IP hosta, wersję komponentu Oprogramowania, który przeprowadził kategoryzację, metodę kategoryzacji i zestaw kategorii zdefiniowany dla zasobu internetowego;
- informacje o oprogramowaniu zainstalowanym na Komputerze: nazwy aplikacji i producentów oprogramowania, klucze rejestru i ich wartości, informacje o plikach zainstalowanych komponentów oprogramowania (sumy kontrolne (MD5, SHA2-256, SHA1), nazwa, ścieżka do pliku na Komputerze, rozmiar, wersja i podpis cyfrowy);
- informacje o stanie antywirusowej ochrony Komputera: wersje i znaczniki czasu publikacji używanych antywirusowych baz danych, identyfikator zadania i identyfikator Oprogramowania, które przeprowadza skanowanie;
- informacje o plikach pobieranych przez Użytkownika Końcowego: adresy URL i IP pobrań i stron pobierania, identyfikator protokołu pobierania i numer portu połączenia, status złośliwości lub braku złośliwości adresu URL, atrybuty, rozmiar i sumy kontrolne plików (MD5, SHA2-256, SHA1), informacje o procesie, który pobrał plik (sumy kontrolne (MD5, SHA2-256, SHA1), datę i czas utworzenia/zbudowania, status automatycznego uruchamiania, atrybuty, nazwy programów pakujących, informacje o sygnaturach, znacznik, identyfikator formatu i entropię pliku wykonywalnego), nazwę pliku i jego ścieżkę na Komputerze, podpis cyfrowy pliku i znacznik czasu jego utworzenia, adres URL miejsca wykrycia, numer skryptu na podejrzanej lub szkodliwej stronie, informacje o wygenerowanych żądaniach HTTP i odpowiedzi na nie;
- informacje o uruchomionych aplikacjach i ich modułach: dane o procesach działających w systemie (identyfikator procesu (PID), nazwę procesu, informacje o koncie, z którego proces został uruchomiony, aplikację i polecenie, które uruchomiły proces, znacznik zaufanego programu lub procesu, pełną ścieżkę plików procesu i ich sum kontrolnych (MD5, SHA2-256, SHA1) oraz uruchamianie wiersza polecenia, poziom integralności procesu, opis produktu, do którego należy proces (nazwę produktu i informacje o wydawcy), używane certyfikaty cyfrowe i informacje niezbędne do zweryfikowania ich autentyczności lub informacje o braku podpisu cyfrowego pliku), a także informacje o modułach załadowanych do procesów (ich nazwy, rozmiary, typy, daty utworzenia, atrybuty, sumy kontrolne (MD5, SHA2-256, SHA1), ścieżki na Komputerze), informacje o nagłówku pliku PE, nazwy programów pakujących (jeśli plik był spakowany);
- informacje o wszystkich potencjalnie szkodliwych obiektach i aktywnościach: nazwa wykrytego obiektu i pełna ścieżka dostępu do obiektu na komputerze, sumy kontrolne przetworzonych plików (MD5, SHA2-256, SHA1), data i godzina wykrycia, nazwy i rozmiary zainfekowanych plików i ścieżki dostępu do tych plików, kod szablonu ścieżki dostępu, flaga pliku wykonywalnego, wskaźnik określający, czy obiekt znajduje się w kontenerze, nazwy narzędzi pakujących (jeśli plik został spakowany), kod typu pliku, ID formatu pliku, lista działań wykonanych przez szkodliwe oprogramowanie oraz decyzja podjęta przez oprogramowanie i reakcja użytkownika, identyfikatory antywirusowych baz danych oraz wpisy w tych antywirusowych bazach danych, które zostały użyte do podjęcia decyzji, wskaźnik potencjalnie szkodliwego obiektu, nazwa wykrytego zagrożenia zgodna z klasyfikacją Posiadacza praw, poziom zagrożenia, stan wykrycia i metoda wykrycia, powód włączenia do analizowanego kontekstu i numer sekwencyjny pliku w kontekście, sumy kontrolne (MD5, SHA2-256, SHA1), nazwa i atrybuty pliku wykonywalnego aplikacji, poprzez którą przesłana została zainfekowana wiadomość lub odnośnik, zdepersonalizowane adresy IP (IPv4 i IPv6) hosta zablokowanego obiektu, entropia pliku, wskaźnik automatycznego uruchomienia pliku, godzina pierwszego wykrycia pliku w systemie, liczba uruchomień pliku od ostatniego wysłania statystyk, informacje o nazwie, sumy kontrolne (MD5, SHA2-256, SHA1) oraz rozmiar klienta

poczty, poprzez którego otrzymano szkodliwy obiekt, ID zadania oprogramowania, które przeprowadziło skanowanie, wskaźnik pokazujący, czy podpis lub reputacja pliku zostały sprawdzone, wynik przetworzenia pliku, suma kontrolna (MD5) wzorca zebranego dla obiektu, rozmiar wzorca w bajtach i specyfikacje techniczne zastosowanych technologii wykrywania;

- informacje o skanowanych obiektach: przypisaną grupę zaufania, do której i/lub z której plik został umieszczony, powód, dla którego plik umieszczono w danej kategorii, identyfikator kategorii, informacje o źródle kategorii i wersji bazy danych kategorii, znacznik certyfikatu zaufania pliku, nazwę dostawcy pliku, wersję pliku, nazwę i wersję aplikacji, do której należy plik;
- informacje o wykrytych lukach w zabezpieczeniach: identyfikator luki w bazie danych luk, klasę zagrożenia luki;
- informacje o emulacji pliku wykonywalnego: rozmiar pliku i jego sumy kontrolne (MD5, SHA2-256, SHA1), wersję komponentu emulatora, głębokość emulacji, tablicę właściwości bloków logicznych i funkcji w obrębie bloków logicznych uzyskanych podczas emulacji oraz dane z nagłówków PE pliku wykonywalnego;
- adresy IP atakującego komputera (IPv4 i IPv6), numer portu na Komputerze będącym celem ataku sieciowego, identyfikator protokołu pakietu IP zawierającego atak, cel ataku (nazwę organizacji, stronę internetową), znacznik reakcji na atak, wagę ataku, poziom zaufania;
- informacje o atakach powiązanych ze sfalszowanymi zasobami sieciowymi, adresy DNS i IP (IPv4 i IPv6) odwiedzonych stron internetowych;
- adresy DNS i IP (IPv4 lub IPv6) zażądanego zasobu sieciowego, informacje o pliku i kliencie sieci Web uzyskujących dostęp do zasobu sieciowego, nazwę, rozmiar i sumy kontrolne (MD5, SHA2-256, SHA1) pliku, pełną ścieżkę do pliku oraz kod szablonu ścieżki, wynik weryfikacji jego podpisu cyfrowego i jego stan w KSN;
- informacje o wycofaniu szkodliwych działań: dane dotyczące pliku, którego aktywność została wycofana (nazwa pliku, pełna ścieżka dostępu do pliku, jego rozmiar i sumy kontrolne (MD5, SHA2-256, SHA1)), dane dotyczące pomyślnych i niepomyślnych działań mających na celu usunięcie, zmianę nazwy i skopiowanie plików oraz przywrócenie wartości w rejestrze (nazwy kluczy rejestru i ich wartości) oraz informacje o plikach systemowych zmodyfikowanych przez szkodliwe oprogramowanie, przed i po wycofaniu działań;
- informacje o wyłączeniach ustawionych dla komponentu Adaptacyjna kontrola anomalii: identyfikator i status reguły, która została wyzwolona, czynność wykonywaną przez Oprogramowanie podczas wyzwolania reguły, rodzaj konta użytkownika, w ramach którego proces lub wątek wykonuje podejrzaną aktywność, informacje o procesie, który był przedmiotem podejrzanego aktywności (identyfikator skryptu lub nazwa pliku procesu, pełna ścieżka do pliku procesu, kod szablonu ścieżki, sumy kontrolne (MD5, SHA2-256, SHA1) pliku procesu); informacje o obiekcie, który wykonał podejrzanego aktywności, jak również o obiekcie, który był przedmiotem podejrzanego aktywności (nazwa klucza rejestru lub nazwa pliku, pełna ścieżka do pliku, kod szablonu ścieżki oraz sumy kontrolne (MD5, SHA2-256, SHA1) pliku);
- informacje o załadowanych modułach oprogramowania: nazwa, rozmiar i sumy kontrolne (MD5, SHA2-256, SHA1) pliku modułu, pełna ścieżka dostępu do niego oraz kod szablonu ścieżki dostępu, ustawienia podpisu cyfrowego pliku modułu, data i godzina utworzenia podpisu, nazwa podmiotu i organizacji, która podpisała plik modułu, ID procesu, w którym moduł został załadowany, nazwa dostawcy modułu oraz numer sekwencyjny modułu w kolejce ładowania;
- informacje o jakości interakcji Oprogramowania z usługami KSN: datę i godzinę rozpoczęcia i zakończenia okresu, w którym generowane były statystyki, informacje o jakości żądań i połączeniu z każdą z wykorzystywanych usług KSN (identyfikator usługi KSN, liczba udanych żądań, liczba żądań z odpowiedziami z pamięci podręcznej, liczba nieudanych żądań (problemy sieciowe, wyłączenie KSN w ustawieniach Oprogramowania, nieprawidłowe przekierowanie), rozłożenie w czasie udanych żądań, rozkład w czasie anulowanych żądań, rozkład w czasie żądań z przekroczonym limitem czasu, liczbę połączeń do KSN pobranych z pamięci podręcznej, liczbę udanych połączeń do KSN, liczbę nieudanych połączeń do KSN, liczbę udanych transakcji, liczbę nieudanych transakcji, rozkład w czasie udanych połączeń do KSN, rozkład w czasie nieudanych połączeń do KSN, rozkład w czasie udanych transakcji, rozkład w czasie nieudanych transakcji);

- informacje na temat danych w pamięci procesów w przypadku usunięcia potencjalnie złośliwego obiektu: elementy hierarchii obiektów systemu (ObjectManager), dane w pamięci UEFI BIOS oraz nazwy kluczy rejestru i ich wartości;
- informacje o zdarzeniach w dziennikach systemowych: znacznik czasu zdarzenia, nazwa dziennika, w którym znaleziono zdarzenie, typ i kategoria zdarzenia oraz nazwa źródła zdarzenia i opis zdarzenia;
- informacje o połączeniach sieciowych: wersja i sumy kontrolne (MD5, SHA2-256, SHA1) pliku, z którego uruchomiono proces, który otworzył port, ścieżka do pliku procesu i jego podpis cyfrowy, lokalne i zdalne adresy IP, numery lokalnych i zdalnych portów połączeń, stan połączenia oraz znacznik czasu otwarcia portu;
- informacje o dacie instalacji i aktywacji Oprogramowania na Komputerze: ID partnera, który sprzedał licencję, numer seryjny licencji, podpisany nagłówek zgłoszenia z usługi aktywacji (ID regionalnego centrum aktywacji, suma kontrolna kodu aktywacyjnego, suma kontrolna zgłoszenia, data utworzenia zgłoszenia, unikatowy ID zgłoszenia, wersja zgłoszenia, stan licencji, data i godzina rozpoczęcia/zakończenia zgłoszenia, unikatowy ID licencji, wersja licencji), ID certyfikatu użytego do podpisania nagłówka zgłoszenia, suma kontrolna (MD5) pliku klucza, unikatowy ID instalacji Oprogramowania na Komputerze, typ i ID aplikacji, która jest aktualizowana, ID zadania aktualizacji;
- informacje o zestawie wszystkich zainstalowanych aktualizacji oraz zestawie ostatnio zainstalowanych/usuniętych aktualizacji, typ zdarzenia, które spowodowało przesłanie informacji o aktualizacji, czas od instalacji ostatniej aktualizacji oraz informacje o wszelkich aktualnie zainstalowanych antywirusowych bazach danych;
- informacje o działaniu oprogramowania na komputerze: dane dotyczące użycia procesora, dane dotyczące użycia pamięci (Bajty prywatne, Pula niestronicowana, Pula stronicowana), liczba aktywnych wątków w procesie oprogramowania i oczekujące wątki, a także czas działania oprogramowania przed wystąpieniem błędu;
- liczbę zrzutów oprogramowania i zrzutów systemu (BSOD - niebieski ekran śmierci) od momentu zainstalowania Oprogramowania oraz od momentu ostatniej aktualizacji, identyfikator i wersję modułu Oprogramowania, który uległ awarii, stos pamięci w procesie Oprogramowania oraz informacje o antywirusowych bazach danych w momencie awarii;
- dane na temat zrzutu systemu (BSOD - niebieski ekran śmierci): znacznik wskazujący wystąpienie niebieskiego ekranu na Komputerze, nazwę sterownika, który spowodował wystąpienie niebieskiego ekranu, adres i stos pamięci w sterowniku, znacznik wskazujący czas trwania sesji systemu operacyjnego przed wystąpieniem niebieskiego ekranu, stos pamięci sterownika, który uległ awarii, typ przechowywanego zrzutu pamięci, znacznik sesji systemu operacyjnego informujący o trwaniu jego sesji przez ponad 10 minut przed wystąpieniem niebieskiego ekranu, unikatowy identyfikator zrzutu oraz znacznik czasu niebieskiego ekranu;
- informacje o błędach lub problemach z wydajnością, które wystąpiły podczas pracy komponentów Oprogramowania: identyfikator stanu Oprogramowania, typ błędu, kod i przyczynę oraz czas wystąpienia błędu, identyfikatory komponentu, modułu i procesu produktu, w którym wystąpił błąd, identyfikator zadania lub kategorii aktualizacji, w której wystąpił błąd, rejestry sterowników wykorzystywanych przez Oprogramowanie (kod błędu, nazwa modułu, nazwa pliku źródłowego oraz linia, w której wystąpił błąd);
- informacje o aktualizacjach antywirusowych baz danych i składników Oprogramowania: nazwę, datę i godzinę indeksowania plików pobranych podczas ostatniej aktualizacji i pobieranych podczas bieżącej aktualizacji;
- informacje o nieprawidłowym zakończeniu działania Oprogramowania: znacznik czasu utworzenia zrzutu, jego typ, typ zdarzenia, które spowodowało nieprawidłowe zakończenie działania Oprogramowania (nieoczekiwanego wyłączenia zasilania, awarii aplikacji innej firmy) oraz datę i czas nieoczekiwanego wyłączenia zasilania;
- informacje o kompatybilności sterowników Oprogramowania ze sprzętem i Oprogramowaniem: informacje o właściwościach systemu operacyjnego ograniczających funkcjonalność komponentów Oprogramowania (Secure Boot, KPTI, WHQL Enforce, BitLocker, Case Sensitivity), typ zainstalowanego Oprogramowania do pobrania (UEFI, BIOS), identyfikator modułu Trusted Platform Module (TPM), wersję specyfikacji TPM, informacje o procesorze zainstalowanym w Komputerze, tryb pracy i parametry Code Integrity i Device Guard, tryb pracy

sterowników i powód korzystania z aktualnego trybu, wersję sterowników Oprogramowania, status obsługi wirtualizacji oprogramowania i sprzętu Komputera;

- informacje o aplikacjach innych firm, które spowodowały błąd: ich nazwy, wersje i lokalizacje, kod błędu i informacje o błędzie z dziennika systemowego aplikacji, adres błędu i stos pamięci aplikacji innej firmy, znacznik wskazujący wystąpienie błędu w komponencie Oprogramowania, czas działania aplikacji innej firmy przed wystąpieniem błędu, sumy kontrolne (MD5, SHA2-256, SHA1) obrazu procesu aplikacji, w którym wystąpił błąd, ścieżkę obrazu procesu aplikacji i kod szablonu ścieżki, informację z dziennika systemowego z opisem błędu powiązanego z aplikacją, informacje o module aplikacji, w którym wystąpił błąd (identyfikator wyjątku, adres pamięci związany z awarią jako przesunięcie w module aplikacji, nazwę i wersję modułu, identyfikator awarii aplikacji we wtyczce Posiadacza Praw i stos pamięci z awarii, a także czas trwania sesji aplikacji przed awarią);
- wersję komponentu aktualizującego Oprogramowania, liczbę awarii komponentu aktualizującego w czasie trwania zadań aktualizacji przez łączny czas działania komponentu, identyfikator typu zadania aktualizacji, liczbę nieudanych prób ukończenia zadań aktualizacji przez komponent aktualizujący;
- informacje o działaniu komponentów monitorujących system Oprogramowania: pełne wersje komponentów, datę i godzinę uruchomienia komponentów, kod zdarzenia, które przepełniło kolejkę zdarzeń i liczbę takich zdarzeń, całkowitą liczbę zdarzeń przepełnienia kolejki, informacje o pliku procesu inicjatora zdarzenia (nazwę pliku i jego ścieżkę na Komputerze, kod szablonu ścieżki pliku, sumy kontrolne (MD5, SHA2-256, SHA1) procesu związanego z plikiem, wersję pliku), identyfikator przechwycenia zdarzenia, pełną wersję filtra przechwytyującego, identyfikator typu przechwyconego zdarzenia, wielkość kolejki zdarzeń i liczbę zdarzeń pomiędzy pierwszym zdarzeniem w kolejce a bieżącym zdarzeniem, liczbę zaległych zdarzeń w kolejce, informacje o pliku procesu inicjatora bieżącego zdarzenia (nazwę pliku i jego ścieżkę na Komputerze, kod szablonu ścieżki pliku, sumy kontrolne (MD5, SHA2-256, SHA1) procesu związanego z plikiem), czas trwania przetwarzania zdarzenia, maksymalny czas przetwarzania zdarzenia, prawdopodobieństwo wysłania statystyk, informacje o zdarzeniach w systemie operacyjnym, dla których przekroczony został limit czasu przetwarzania (datę i czas zdarzenia, liczbę powtórzeń inicjalizacji antywirusowych baz danych, datę i godzinę ostatniej powtórzonej inicjalizacji antywirusowych baz danych po ich aktualizacji, czas opóźnienia przetwarzania zdarzeń dla każdego komponentu monitorującego system, liczbę zdarzeń oczekujących w kolejce, liczbę przetwarzanych zdarzeń, liczbę opóźnionych zdarzeń bieżącego typu, całkowity czas opóźnienia dla zdarzeń bieżącego typu, całkowity czas opóźnienia dla wszystkich zdarzeń);
- informacje z narzędzia śledzenia zdarzeń Windows (Event Tracing for Windows, ETW) w przypadku problemów z wydajnością Oprogramowania, dostawców zdarzeń SysConfig / SysConfigEx / WinSATAssessment firmy Microsoft: informacje o Komputerze (model, producent, rozmiary obudowy, wersję), informacje o metrykach wydajności systemu Windows (oceny WinSAT, indeks wydajności systemu Windows), nazwę domeny, informacje o procesorach fizycznych i logicznych (liczbę procesorów fizycznych i logicznych, producenta, model, poziom taktowania procesora, liczbę rdzeni, częstotliwość zegara, CPUID, charakterystykę pamięci podręcznej, charakterystykę procesora logicznego, wskaźniki obsługiwanych trybów i instrukcji), informacje o modułach RAM (typ, współczynnik kształtu, producenta, model, pojemność, ziarnistość alokacji pamięci), informacje o interfejsach sieciowych (adresy IP i MAC, nazwę, opis, konfigurację interfejsów sieciowych, podział liczby i wielkości pakietów sieciowych według typu, prędkość wymiany danych w sieci, podział liczby błędów sieciowych według typu), konfigurację kontrolera IDE, adresy IP serwerów DNS, informacje o karcie graficznej (model, opis, producenta, kompatybilność, pojemność pamięci wideo, uprawnienia ekranu, liczbę bitów na piksel, wersję BIOS), informacje o urządzeniach typu plug-and-play (nazwę, opis, identyfikator urządzenia [PnP, ACPI]), informacje o dyskach i urządzeniach pamięci masowej (liczbę dysków lub napędów flash, producenta, model, pojemność dysku, liczbę cylindrów, liczbę ścieżek na cylinder, liczbę sektorów na ścieżkę, pojemność sektora, charakterystykę pamięci podręcznej, liczbę sekwencyjną, liczbę partycji, konfigurację kontrolera SCSI), informacje o dyskach logicznych (numer sekwencyjny, pojemność partycji, pojemność wolumenu, literę wolumenu, typ partycji, typ systemu plików, liczbę klastrów, wielkość klastra, liczbę sektorów na klastr, liczbę pustych i zajętych klastrów, literę woluminu rozruchowego, adres przesunięcia partycji w stosunku do początku dysku), informacje o BIOS-ie płyty głównej (producenta, datę publikacji, wersję), informacje o płycie głównej (producenta, model, typ), informacje o pamięci fizycznej (współdzielonej i wolnej pojemności), informacje o usługach systemu operacyjnego (nazwę, opis, status, znacznik, informacje o procesach [nazwę i PID]), parametry zużycia energii dla Komputera, konfigurację kontrolera przerwań, ścieżkę do folderów systemu Windows (Windows i System32), informacje o systemie operacyjnym (wersję, kompilację, datę wydania, nazwę, typ, datę instalacji), rozmiar pliku stronicowania, informacje o monitorach (liczbę, producenta, zezwolenia ekranu, rozdzielczość, typ), informacje o sterowniku karty graficznej (producenta, datę wydania, wersję);

- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń EventTrace / EventMetadata firmy Microsoft: informacje o kolejności zdarzeń systemowych (typ, godzinę, datę, strefę czasową), metadane o pliku z wynikami śledzenia (nazwę, strukturę, parametry śledzenia, rozbięcie liczby operacji śledzenia według typu), informacje o systemie operacyjnym (nazwę, typ, wersję, kompilację, datę wydania, godzinę uruchomienia);
- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń Process / Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power firmy Microsoft: informacje o rozpoczętych i zakończonych procesach (nazwę, PID, parametry uruchamiania, wiersz poleceń, kod zwrotny, parametry zarządzania energią, czas uruchomienia i zakończenia, typ tokena dostępu, SID, SessionID, liczbę zainstalowanych deskryptorów), informacje o zmianach priorytetów wątków (TID, priorytet, czas), informacje o operacjach dyskowych procesu (typ, czas, pojemność, liczbę), historię zmian w strukturze i pojemności procesów dostępnej pamięci;
- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń StackWalk / Perfinfo firmy Microsoft: informacje o licznikach wydajności (wydajność poszczególnych sekcji kodu, kolejność wywołań funkcji, PID, TID, adresy i atrybuty ISR i DPC);
- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń KernelTraceControl-ImageID firmy Microsoft: informacje o plikach wykonywalnych i bibliotekach dynamicznych (nazwę, rozmiar obrazu, pełną ścieżkę), informacje o plikach PDB (nazwę, identyfikator), dane zasobu VERSIONINFO dla plików wykonywalnych (nazwę, opis, twórcę, lokalizację, wersję i identyfikator aplikacji, wersję i identyfikator pliku);
- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń FileIo / DiskIo / Image / Windows Kernel Disk firmy Microsoft: informacje o operacjach na plikach i dyskach (typ, pojemność, czas uruchomienia, czas zakończenia, czas trwania, status zakończenia, PID, TID, adresy wywołania funkcji sterownika, I/O Request Packet (IRP), atrybuty obiektu pliku Windows), informacje o plikach związanych z operacjami na plikach i na dyskach (nazwę, wersję, rozmiar, pełną ścieżkę, atrybuty, przesunięcie, sumę kontrolną obrazu, opcje otwarcia i dostępu);
- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń PageFault firmy Microsoft: informacje na temat błędów dostępu do strony pamięci (adres, czas, pojemność, PID, TID, atrybuty obiektu pliku Windows, parametry alokacji pamięci);
- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń Thread firmy Microsoft: informacje o tworzeniu/ukończeniu wątków, informacje o uruchomionych wątkach (PID, TID, rozmiar stosu, priorytety i alokację zasobów CPU, zasoby I/O, strony pamięci pomiędzy wątkami, adres stosu, adres funkcji inicjującej, adres bloku środowiska Thread Environment Block (TEB), znacznik usługi Windows);
- informacje z narzędzia śledzenia zdarzeń Windows (ETW), dostawców zdarzeń Microsoft Windows Kernel Memory firmy Microsoft: informacje o operacjach zarządzania pamięcią (stan zakończenia, czas, liczbę, PID), strukturę alokacji pamięci (typ, pojemność, SessionID, PID);
- informacje o działaniu Oprogramowania w przypadku problemów z wydajnością: identyfikator instalacji Oprogramowania, typ i wartość spadku wydajności, informacje o sekwencji zdarzeń w ramach Oprogramowania (czas, strefę czasową, typ, stan zakończenia, identyfikator komponentu Oprogramowania, identyfikator scenariusza działania Oprogramowania, TID, PID, adresy wywołań funkcji), informacje o połączeniach sieciowych do sprawdzenia (URL, kierunek połączenia, rozmiar pakietu sieciowego), informacje o plikach PDB (nazwę, identyfikator, rozmiar obrazu pliku wykonywalnego), informacje o plikach do sprawdzenia (nazwę, pełną ścieżkę, sumę kontrolną), parametry monitorowania wydajności Oprogramowania;
- informacje o ostatnim nieudanym ponownym uruchomieniu systemu operacyjnego: liczbę nieudanych prób ponownego uruchomienia od momentu instalacji systemu operacyjnego, dane na temat zrzutu systemu (kod i parametry błędu, nazwę, wersję i sumę kontrolną (CRC32) modułu, który spowodował błąd działania systemu operacyjnego, adres błędu jako przesunięcie w module, sumy kontrolne (MD5, SHA2-256, SHA1) zrzutu systemu);
- informacje pozwalające zweryfikować autentyczność certyfikatów cyfrowych używanych do podpisywania plików: odcisk palca certyfikatu, algorytm sumy kontrolnej, klucz publiczny i numer seryjny certyfikatu, nazwę wystawcy certyfikatu, wynik weryfikacji certyfikatu i identyfikator bazy danych certyfikatu;

- informacje o procesie uruchamiającym atak na mechanizm autoochrony Oprogramowania: nazwę i rozmiar pliku procesu, jego sumy kontrolne (MD5, SHA2-256, SHA1), pełną ścieżkę pliku procesu i kod szablonu ścieżki pliku, znaczniki czasu utworzenia/zbudowania, znacznik pliku wykonywalnego, atrybuty pliku procesu, informacje o certyfikacie użytym do podpisania pliku procesu, kod konta użytego do uruchomienia procesu, identyfikator operacji wykonanych w celu uzyskania dostępu do procesu, typ zasobu, za pomocą którego operacja jest wykonywana (proces, plik, obiekt rejestru, funkcja wyszukiwania FindWindow), nazwę zasobu, za pomocą którego operacja jest wykonywana, znacznik wskazujący powodzenie operacji, status pliku procesu i jego sygnaturę według KSN;
- informacje o Oprogramowaniu Posiadacza praw: pełna wersja, typ, lokalizacja i stan działania używanego Oprogramowania, wersje zainstalowanych komponentów Oprogramowania i stanu ich działania, informacje o zainstalowanych aktualizacjach Oprogramowania, wartość filtra TARGET, wersja protokołu użytego do nawiązania połączenia z usługami Posiadacza praw;
- informacje o sprzęcie zainstalowanym na Komputerze: typ, nazwę, nazwę modelu, wersję oprogramowania układowego, parametry urządzeń wbudowanych i podłączonych, unikatowy identyfikator Komputera z zainstalowanym Oprogramowaniem;
- informacje o wersjach systemu operacyjnego i zainstalowanych aktualizacji, długość słowa, edycję i parametry trybu uruchamiania systemu operacyjnego oraz wersję i sumy kontrolne (MD5, SHA2-256, SHA1) pliku jądra systemu operacyjnego, a także datę i godzinę uruchomienia systemu operacyjnego;
- pliki wykonywalne i niewykonywalne, całkowicie lub częściowo;
- części pamięci RAM Komputera;
- sektory zaangażowane w proces rozruchu systemu operacyjnego;
- pakiety danych dotyczące ruchu sieciowego;
- strony internetowe i wiadomości e-mail zawierające podejrzane i szkodliwe obiekty;
- opis klas i instancji klas repozytorium WMI;
- raporty dotyczące aktywności aplikacji:
 - nazwę, rozmiar i wersję przesyłanego pliku, jego opis i sumy kontrolne (MD5, SHA2-256, SHA1), identyfikator formatu pliku, nazwę dostawcy pliku, nazwę produktu, do którego należy plik, pełną ścieżkę do pliku na Komputerze, kod szablonu ścieżki, znaczniki czasu utworzenia i modyfikacji pliku;
 - datę/godzinę rozpoczęcia i zakończenia okresu ważności certyfikatu (jeśli plik posiada podpis cyfrowy), datę i godzinę podpisu, nazwę wystawcy certyfikatu, informacje o właścicielu certyfikatu, odcisk palca, klucz publiczny certyfikatu i odpowiednie algorytmy oraz numer seryjny certyfikatu;
 - nazwę konta, z którego proces został uruchomiony;
 - sumy kontrolne (MD5, SHA2-256, SHA1) nazwy Komputera, na którym proces jest uruchomiony;
 - tytuły okien procesów;
 - Identyfikator antywirusowych baz danych, nazwa wykrytego zagrożenia według klasyfikacji Posiadacza praw;
 - dane na temat zainstalowanej licencji, jej identyfikator, typ i datę wygaśnięcia;
 - lokalny czas Komputera w momencie dostarczenia informacji;
 - nazwy i ścieżki plików, do których proces uzyskał dostęp;

- nazwy i wartości kluczy rejestru, do których proces uzyskał dostęp;
- adresy URL i IP, do których proces uzyskał dostęp;
- adresy URL i IP, z których pobrano uruchomiony plik.

Przekazywanie danych podczas korzystania z rozwiązań Detection and Response

Na komputerach z zainstalowanym programem Kaspersky Endpoint Security przechowywane są dane przygotowane do automatycznego wysłania na serwery [Kaspersky Endpoint Detection and Response](#) i [Kaspersky Sandbox](#). Pliki są przechowywane na komputerach w zwykłej, niezaszyfrowanej formie.

Określony zestaw danych jest zależny od rozwiązania, w ramach którego używana jest aplikacja Kaspersky Endpoint Security.

Aktywowanie Kaspersky Endpoint Detection and Response

Wszystkie dane, które aplikacja przechowuje lokalnie na komputerze, są usuwane z komputera podczas odinstalowywania Kaspersky Endpoint Security.

Dane otrzymane w wyniku wykonania zadania Skanowanie IOC (zadanie standardowe)

Kaspersky Endpoint Security automatycznie przesyła dane wyników wykonania zadania *Skanowanie IOC* do Kaspersky Security Center.

Dane uwzględnione w wynikach wykonania zadania *Skanowanie IOC* mogą zawierać następujące informacje:

- Adres IP z tablicy ARP
- Adres fizyczny z tablicy ARP
- Typ i nazwa rekordu DNS
- Adres IP chronionego komputera
- Adres fizyczny (adres MAC) chronionego komputera
- Identyfikator uwzględniony we wpisie dziennika zdarzeń
- Nazwa źródła danych zapisana w dzienniku
- Nazwa dziennika
- Czas zdarzenia
- Skrót MD5 i SHA256 pliku

- Pełna nazwa pliku (łącznie ze ścieżką)
- Rozmiar pliku
- Zdalny adres IP i port, z którym nawiązano połączenie podczas skanowania
- Adres IP lokalnej karty sieciowej
- Port otwarty na lokalnej karcie sieciowej
- Numer protokołu (zgodnie ze standardem IANA)
- Nazwa procesu
- Argumenty procesu
- Ścieżka do pliku procesu
- Identyfikator procesu (PID) systemu Windows
- Identyfikator procesu nadrzędnego (PID) systemu Windows
- Konto użytkownika, które rozpoczęło proces
- Data i godzina rozpoczęcia procesu
- Nazwa usługi
- Opis usługi
- Ścieżka i nazwa usługi DLL (svchost)
- Ścieżka i nazwa pliku wykonywalnego usługi
- Identyfikator usługi (PID) systemu Windows
- Typ usługi (na przykład sterownik jądra lub karta sieciowa)
- Stan usługi
- Tryb uruchomienia usługi
- Nazwa konta użytkownika
- Nazwa woluminu
- Litera woluminu
- Typ woluminu
- Wartość rejestru systemu Windows
- Wartość gałęzi rejestru
- Ścieżka klucza rejestru (bez gałęzi i nazwy wartości)

- Ustawienie rejestru
- System (środowisko)
- Nazwa i wersja systemu operacyjnego zainstalowanego na komputerze
- Nazwa sieciowa chronionego komputera
- Domena lub grupa, do której należy chroniony komputer
- Nazwa przeglądarki
- Wersja przeglądarki
- Czas ostatniego dostępu do zasobu internetowego
- Adres URL z żądania HTTP
- Nazwa konta użyta w żądaniu HTTP
- Nazwa pliku procesu, który wykonał żądanie HTTP
- Pełna ścieżka do pliku procesu, który wykonał żądanie HTTP
- Identyfikator procesu (PID) systemu Windows, który wykonał żądanie HTTP
- Strona odsyłająca HTTP (adres URL źródła żądania HTTP)
- Identyfikator URI zasobu żądanego przez HTTP
- Informacje o kliencie użytkownika HTTP (aplikacji, która wysłała żądanie HTTP)
- Czas wykonania żądania HTTP
- Unikalny identyfikator procesu, który wykonał żądanie HTTP

Dane do tworzenia łańcucha rozwoju zagrożeń

Dane do tworzenia łańcucha rozwoju zagrożeń są domyślnie przechowywane przez siedem dni. Dane są automatycznie wysyłane do aplikacji Kaspersky Security Center.

Dane do tworzenia łańcucha rozwoju zagrożeń mogą zawierać następujące informacje:

- Data i godzina incydentu
- Nazwa wykrywania
- Tryb skanowania
- Stan ostatniej akcji związanej z wykrywaniem
- Powód niepowodzenia przetwarzania wykrywania
- Typ wykrytego obiektu

- Nazwa wykrytego obiektu
- Stan zagrożenia po przetworzeniu obiektu
- Powód niepowodzenia wykonywania akcji w odniesieniu do obiektu
- Akcje wykonywane w celu wycofania złośliwych działań
- Informacje o przetwarzanym obiekcie:
 - Unikalny identyfikator procesu
 - Unikalny identyfikator procesu nadrzędnego
 - Unikalny identyfikator pliku procesu
 - Identyfikator procesu systemu Windows (PID)
 - Wiersz polecenia procesu
 - Konto użytkownika, które rozpoczęło proces
 - Kod sesji logowania, w której proces jest uruchomiony
 - Typ sesji, w której proces jest uruchomiony
 - Poziom integralności przetwarzanego obiektu
 - Członkostwo konta użytkownika, które rozpoczęło proces, w uprzywilejowanych grupach lokalnych i domenowych
 - Identyfikator przetwarzanego obiektu
 - Pełna nazwa przetwarzanego obiektu
 - Identyfikator chronionego urządzenia
 - Pełna nazwa obiektu (lokalna nazwa pliku lub adres internetowy pobranego pliku)
 - Skrót MD5 lub SHA256 przetwarzanego obiektu
 - Typ przetwarzanego obiektu
 - Data utworzenia przetwarzanego obiektu
 - Data ostatniej modyfikacji przetwarzanego obiektu
 - Rozmiar przetwarzanego obiektu
 - Atrybuty przetwarzanego obiektu
 - Organizacja sygnująca przetwarzany obiekt
 - Wynik weryfikacji certyfikatu cyfrowego przetwarzanego obiektu
 - Identyfikator zabezpieczeń (SID) przetwarzanego obiektu

- Identyfikator strefy czasowej przetwarzanego obiektu
- Adres internetowy pobierania przetwarzanego obiektu (tylko dla plików na dysku)
- Nazwa aplikacji, która pobrała plik
- Skróty MD5 i SHA256 aplikacji, która pobrała plik
- Nazwa aplikacji, która ostatnio zmodyfikowała plik
- Skróty MD5 i SHA256 aplikacji, która ostatnio zmodyfikowała plik
- Liczba uruchomień przetwarzanego obiektu
- Data i godzina pierwszego uruchomienia przetwarzanego obiektu
- Unikalne identyfikatory pliku
- Pełna nazwa pliku (lokalna nazwa pliku lub adres internetowy pobranego pliku)
- Ścieżka do przetwarzanej zmiennej rejestru systemu Windows
- Nazwa przetwarzanej zmiennej rejestru systemu Windows
- Wartość przetwarzanej zmiennej rejestru systemu Windows
- Typ przetwarzanej zmiennej rejestru systemu Windows
- Wskaźnik członkostwa przetwarzanego klucza rejestru w punkcie automatycznego uruchamiania
- Adres internetowy przetwarzanego żądania internetowego
- Źródło łącza przetwarzanego żądania internetowego
- Klient użytkownika przetwarzanego żądania internetowego
- Typ przetwarzanego żądania internetowego (GET lub POST).
- Lokalny port IP przetwarzanego żądania internetowego
- Zdalny port IP przetwarzanego żądania internetowego
- Kierunek połączenia (przychodzący lub wychodzący) przetwarzanego żądania internetowego
- Identyfikator procesu, w którym osadzono złośliwy kod

Kaspersky Sandbox

All data that the application stores locally on the computer, is deleted from the computer when Kaspersky Endpoint Security is uninstalled.

Dane serwisowe

Kaspersky Endpoint Security przechowuje następujące dane przetwarzane podczas automatycznego reagowania:

- Przetwarzane pliki i dane wprowadzone przez użytkownika podczas konfigurowania wbudowanego agenta Kaspersky Endpoint Security:
 - Pliki poddane kwarantannie
 - Klucz publiczny certyfikatu używanego do zintegrowania z serwerem Kaspersky Sandbox
- Pamięć podręczna wbudowanego agenta Kaspersky Endpoint Security:
 - Czas zapisania wyników skanowania w pamięci podręcznej
 - Skrót MD5 zadania skanowania
 - Identyfikator zadania skanowania
 - Wynik skanowania obiektu
- Kolejka żądań skanowania obiektów:
 - Identyfikator obiektu w kolejce
 - Czas umieszczenia obiektu w kolejce
 - Stan przetwarzania obiektu w kolejce
 - Identyfikator sesji użytkownika w systemie operacyjnym, w którym utworzono zadanie skanowania obiektów
 - Identyfikator systemu (SID) użytkownika systemu operacyjnego, którego konto zostało użyte do utworzenia zadania
 - Skrót MD5 zadania skanowania obiektów
- Informacje o zadaniach, dla których wbudowany agent Kaspersky Endpoint Security oczekuje na wyniki skanowania z serwera Kaspersky Sandbox:
 - Godzina odebrania zadania skanowania obiektu
 - Stan przetwarzania obiektu
 - Identyfikator sesji użytkownika w systemie operacyjnym, w którym utworzono zadanie skanowania obiektów
 - Identyfikator zadania skanowania obiektów
 - Skrót MD5 zadania skanowania obiektów
 - Identyfikator systemu (SID) użytkownika systemu operacyjnego, którego konto zostało użyte do utworzenia zadania
 - Schemat XML automatycznie tworzonego wskaźnika IOC
 - Skrót MD5 lub SHA256 skanowanego obiektu

- Błędy przetwarzania
- Nazwy obiektów, dla których utworzono zadanie
- Wynik skanowania obiektu

Dane uwzględnione w żądaniach kierowanych do serwera Kaspersky Sandbox

Następujące dane z żądań z wbudowanego agenta Kaspersky Endpoint Security do Kaspersky Sandbox są przechowywane lokalnie na komputerze:

- Skrót MD5 zadania skanowania
- Identyfikator zadania skanowania
- Zeskanowany obiekt i wszystkie powiązane pliki

Dane otrzymane w wyniku wykonania zadania Skanowanie IOC (zadanie autonomiczne)

Kaspersky Endpoint Security automatically submits data on the *Skanowanie IOC* task execution results to Kaspersky Security Center.

Dane uwzględnione w wynikach wykonania zadania skanowania IOC mogą zawierać następujące informacje:

- Adres IP z tablicy ARP
- Adres fizyczny z tablicy ARP
- Typ i nazwa rekordu DNS
- Adres IP chronionego urządzenia
- Adres fizyczny (adres MAC) chronionego urządzenia
- Identyfikator uwzględniony we wpisie dziennika zdarzeń
- Nazwa źródła danych zapisana w dzienniku
- Nazwa dziennika
- Czas zdarzenia
- Skrót MD5 i SHA256 obiektów
- Pełna nazwa pliku (łącznie ze ścieżką)
- Rozmiar pliku
- Zdalny adres IP, z którym nawiązano połączenie podczas skanowania
- Adres IP lokalnej karty sieciowej
- Port otwarty na lokalnej karcie sieciowej

- Numer protokołu (zgodnie ze standardem IANA)
- Nazwa procesu
- Argumenty procesu
- Ścieżka do pliku procesu
- Identyfikator procesu (PID) systemu Windows
- Identyfikator procesu nadrzędnego (PID) systemu Windows
- Konto użytkownika, które rozpoczęło proces
- Data i godzina rozpoczęcia procesu
- Nazwa usługi
- Opis usługi
- Ścieżka i nazwa usługi DLL (svchost)
- Ścieżka i nazwa pliku wykonywalnego usługi
- Identyfikator usługi (PID) systemu Windows
- Typ usługi (na przykład sterownik jądra lub karta sieciowa)
- Stan usługi
- Tryb uruchomienia usługi
- Nazwa konta użytkownika
- Nazwa woluminu
- Litera woluminu
- Typ woluminu
- Wartość rejestru systemu Windows
- Wartość gałęzi rejestru
- Ścieżka klucza rejestru (bez gałęzi i nazwy wartości)
- Ustawienie rejestru
- System (środowisko)
- Nazwa i wersja systemu operacyjnego zainstalowanego na urządzeniu
- Nazwa sieciowa chronionego urządzenia
- Domena lub grupa, do której należy chronione urządzenie

- Nazwa przeglądarki
- Wersja przeglądarki
- Czas ostatniego dostępu do zasobu internetowego
- Adres URL z żądania HTTP
- Nazwa konta użyta w żądaniu HTTP
- Nazwa pliku procesu, który wykonał żądanie HTTP
- Pełna ścieżka do pliku procesu, który wykonał żądanie HTTP
- Identyfikator procesu (PID) systemu Windows, który wykonał żądanie HTTP
- Strona odsyłająca HTTP (adres URL źródła żądania HTTP)
- Identyfikator URI zasobu żądanego przez HTTP
- Informacje o kliencie użytkownika HTTP (aplikacji, która wysłała żądanie HTTP)
- Czas wykonania żądania HTTP
- Unikalny identyfikator procesu, który wykonał żądanie HTTP

Zgodność z prawem Unii Europejskiej (RODO)

Kaspersky Endpoint Security może przysyłać dane do Kaspersky w następujących scenariuszach:

- Korzystanie z Kaspersky Security Network.
- Aktywowanie aplikacji przy użyciu kodu aktywacyjnego.
- Aktualizowanie modułów i antywirusowych baz danych aplikacji.
- Otwieranie odnośników w interfejsie aplikacji.
- Zapisywanie zrzutu pamięci.

Niezależnie od klasyfikacji danych i terytorium, z którego dane są otrzymywane, firma Kaspersky stosuje się do najwyższych standardów bezpieczeństwa danych i wdraża różne prawne, organizacyjne i techniczne środki ochrony danych użytkowników, aby zagwarantować bezpieczeństwo i poufność danych, a także żeby zapewnić przestrzeganie praw użytkowników zagwarantowanych przez obowiązujące prawo. Treść Polityki prywatności jest dostępna w [pakiecie dystrybucyjnym aplikacji](#) oraz na [stronie internetowej Kaspersky](#).

Zanim zaczniesz korzystać z Kaspersky Endpoint Security uważnie przeczytaj opis przesyłanych danych w [Umowie licencyjnej](#) i w [Oświadczeniu Kaspersky Security Network](#). Jeśli określone dane przesyłane z Kaspersky Endpoint Security zgodnie z jednym z wyżej opisanych scenariuszy można zaklasyfikować jako dane osobowe zgodnie z prawem lokalnym lub standardowym, musisz upewnić się, że takie dane są przetwarzane zgodnie z prawem i uzyskać zgodę użytkowników końcowych na gromadzenie i przesyłanie tych danych.

Przeczytaj Umowę licencyjną i odwiedź [stronę internetową Kaspersky](#), aby dowiedzieć się więcej o otrzymywaniu, przetwarzaniu, przechowywaniu i niszczeniu przez Kaspersky informacji dotyczących korzystania z aplikacji po zaakceptowaniu Umowy licencyjnej i Oświadczenia Kaspersky Security Network. Pliki license.txt i ksn_<ID języka>.txt zawierają treść Umowy licencyjnej i Oświadczenia Kaspersky Security Network i można je znaleźć w [pakiecie dystrybucyjnym](#) aplikacji.

Jeśli nie chcesz przesyłać danych do Kaspersky, możesz wyłączyć dostarczanie danych.

Korzystanie z Kaspersky Security Network

Korzystając z Kaspersky Security Network, możesz wyrazić zgodę na automatyczne dostarczanie danych wymienionych w [Oświadczeniu Kaspersky Security Network](#). Jeśli nie wyrażasz zgody na dostarczenie tych danych do Kaspersky, użyj Private KSN lub [wyłącz korzystanie z KSN](#). Więcej informacji o Prywatnej sieci KSN można znaleźć w *dokumentacji do Kaspersky Private Security Network*.

Aktywowanie aplikacji przy użyciu kodu aktywacyjnego

Korzystając z kodu aktywacyjnego, wyrażasz zgodę na automatyczne dostarczanie danych wymienionych w [Umowie licencyjnej](#). Jeśli nie zgadzasz się na przesłanie tych danych do Kaspersky, użyj [pliku klucza do aktywacji Kaspersky Endpoint Security](#).

Aktualizowanie modułów i antywirusowych baz danych aplikacji

Korzystając z serwerów Kaspersky, wyrażasz zgodę na automatyczne dostarczanie danych wymienionych w [Umowie licencyjnej](#). Kaspersky wymaga tych informacji do sprawdzenia, czy Kaspersky Endpoint Security jest używany legalnie. Jeśli nie wyrażasz zgody na dostarczenie tych informacji do Kaspersky, użyj [Kaspersky Security Center do aktualizacji baz danych](#) lub [Kaspersky Update Utility](#).

Otwórz odnośniki w interfejsie aplikacji

Korzystając z odnośników w interfejsie aplikacji, wyrażasz zgodę na automatyczne dostarczanie danych wymienionych w [Umowie licencyjnej](#). Dokładna lista danych przesyłanych w każdym określonym odnośniku zależy od miejsca, w którym odnośnik się znajduje w interfejsie aplikacji, a także od problemu, który ma zostać rozwiązany. Jeśli nie wyrażasz zgody na dostarczenie tych danych do Kaspersky, użyj [uproszczonego interfejsu aplikacji](#) lub [ukryj interfejs aplikacji](#).

Zapisywanie zrzutu pamięci

Jeśli masz [włączoną opcję zapisu zrzutów pamięci](#), Kaspersky Endpoint Security utworzy plik zrzutu pamięci, który będzie zawierał wszelkie dane pamięci z procesów aplikacji w momencie, gdy ten plik zrzutu pamięci został utworzony.

Rozpoczęcie pracy

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

- [Lokalny interfejs aplikacji](#).
- Serwer administracyjny Kaspersky Security Center.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Konsola administracyjna Kaspersky Security Center

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

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

Aby uzyskać więcej informacji na temat zarządzania aplikacją w Kaspersky Security Center, [zapoznaj się z systemem pomocy Kaspersky Security Center](#).

Kaspersky Security Center Web Console i Kaspersky Security Center Cloud Console

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

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

Web Console i Cloud Console umożliwiają wykonywanie następujących czynności:

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

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

Informacje o wtyczce zarządzającej Kaspersky Endpoint Security for Windows

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

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

Wtyczka webowa nie jest instalowana domyślnie w Kaspersky Security Center Web Console. W przeciwieństwie do wtyczki zarządzającej dla Konsoli administracyjnej Kaspersky Security Center, która jest instalowana na stacji roboczej administratora, wtyczka webowa musi zostać zainstalowana na komputerze, na którym jest zainstalowana konsola Kaspersky Security Center Web Console. Funkcjonalność wtyczki webowej jest dostępna dla wszystkich administratorów, którzy mają dostęp do konsoli Web Console w przeglądarce. Możesz przejrzeć listę zainstalowanych wtyczek webowych w interfejsie Web Console: **Ustawienia konsoli** → **Wtyczki**. Więcej informacji na temat kompatybilności wersji wtyczek webowych z Web Console można znaleźć w [pomocy do Kaspersky Security Center](#).

Instalowanie wtyczki webowej

Wtyczkę webową możesz zainstalować w następujący sposób:

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

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

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

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

- Pobierz pakiet dystrybucyjny do Web Console z zewnętrznego źródła.

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

Aktualizowanie wtyczki zarządzającej

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

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

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

Wtyczkę webową możesz zaktualizować w następujący sposób:

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

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

- Zaktualizuj wtyczkę webową z pliku.

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

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

Kwestie specjalne dotyczące pracy z różnymi wersjami wtyczek zarządzających

Możesz zarządzać Kaspersky Endpoint Security poprzez Kaspersky Security Center tylko wtedy, gdy posiadasz wtyczkę zarządzającą, której wersja jest równa lub nowsza niż wersja określona w informacjach dotyczących kompatybilności Kaspersky Endpoint Security z wtyczką zarządzającą. Minimalną wymaganą wersję wtyczki zarządzającej możesz sprawdzić w pliku `installer.ini` znajdującym się w [pakiecie dystrybucyjnym](#).

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

Aktualizowanie wtyczki zarządzającej Kaspersky Endpoint Security 10 for Windows

Jeśli wtyczka zarządzająca Kaspersky Endpoint Security 10 for Windows jest zainstalowana w Konsoli administracyjnej, podczas instalowania wtyczki zarządzającej Kaspersky Endpoint Security 11 for Windows należy uwzględnić następujące kwestie:


- Wtyczka zarządzająca Kaspersky Endpoint Security 10 for Windows nie zostanie usunięta i pozostanie dostępna do działania. Dlatego będziesz miał dostęp do dwóch wtyczek zarządzających o pracy z aplikacjami w wersjach 10 i 11.
- Wtyczka zarządzająca Kaspersky Endpoint Security 11 for Windows nie obsługuje zarządzania Kaspersky Endpoint Security 10 for Windows na komputerach użytkowników.
- Wtyczka zarządzająca Kaspersky Endpoint Security 11 for Windows nie obsługuje elementów (na przykład, zasad lub zadań), które zostały utworzone przy użyciu wtyczki zarządzającej Kaspersky Endpoint Security 10 for Windows.

Możesz użyć Kreatora konwersji zasad i zadań, aby przekonwertować zasady i zadania z wersji 10 do wersji 11. Więcej informacji na temat konwertowania zasad i zadań można znaleźć w [pomocy do Kaspersky Security Center](#).



Aktualizowanie wtyczki zarządzającej Kaspersky Endpoint Security 11 for Windows

Jeśli wtyczka zarządzająca Kaspersky Endpoint Security 11 for Windows jest zainstalowana w Konsoli administracyjnej, podczas instalowania nowej wersji wtyczki zarządzającej Kaspersky Endpoint Security 11 for Windows należy uwzględnić następujące kwestie:

- Poprzednia wersja wtyczki zarządzającej Kaspersky Endpoint Security 11 for Windows zostanie usunięta.
- Nowa wersja wtyczki zarządzającej Kaspersky Endpoint Security 11 for Windows obsługuje zarządzanie poprzednią wersją Kaspersky Endpoint Security 11 for Windows na komputerach użytkowników.
- Możesz użyć nowej wersji wtyczki zarządzającej, aby zmienić ustawienia w zasadach, zadaniach i innych elementach utworzonych przez poprzednią wersję wtyczki zarządzającej.
- W przypadku nowych ustawień nowsza wersja wtyczki zarządzającej stosuje domyślne wartości, gdy profil, profil zasad lub zadanie jest zapisywane po raz pierwszy.

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

Aby poznać nowe możliwości aplikacji, zapoznaj się z Informacjami o kompilacji lub [systemem pomocy aplikacji](#).

- Jeśli nowy parametr został dodany do grupy ustawień w nowej wersji wtyczki zarządzającej, poprzednio zdefiniowany stan atrybutu  /  dla tej grupy ustawień nie zostanie zmieniony.
- Jeśli aktualizujesz wtyczkę zarządzającą do wersji 11.2.0, musisz otworzyć zasadę, aby ją przekonwertować automatycznie. W takiej sytuacji Kaspersky Endpoint Security wyświetli monit o potwierdzenie uczestnictwa w KSN. Jeśli już zaktualizowałeś aplikację do wersji 11.20 na komputerach w swojej organizacji, uczestnictwo w KSN zostanie wyłączone, aż do zaakceptowania warunków uczestnictwa w KSN.

Kwestie specjalne podczas używania zaszyfrowanych protokołów do interakcji z zewnętrznymi usługami

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

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

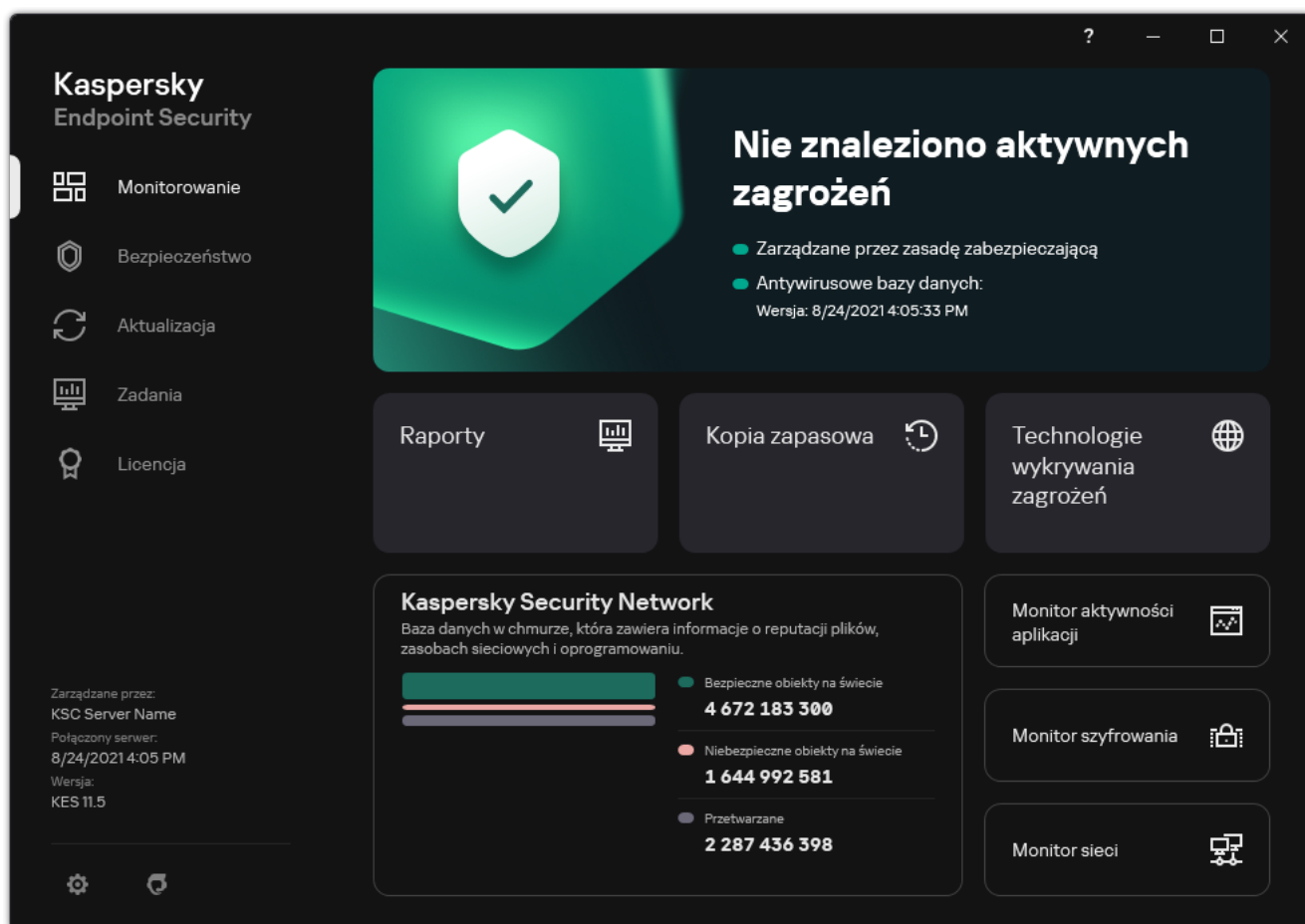
Korzystanie z TLS zabezpiecza aplikację poprzez dostarczenie następujących funkcji:

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

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

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




Interfejs aplikacji



Okno główne aplikacji

Monitorowanie

- **Raporty.** Przeglądaj zdarzenia, które wystąpiły podczas działania aplikacji, pojedynczych modułów i zadań.
- **Kopia zapasowa.** Przeglądaj listę zapisanych kopii zainfekowanych plików, które zostały usunięte przez aplikację.
- **Technologie wykrywania zagrożeń.** Przeglądaj informacje o technologiach wykrywania zagrożeń oraz liczbie zagrożeń wykrytych przez te technologie.
- **Kaspersky Security Network.** Stan połączenia nawiązanego między Kaspersky Endpoint Security a Kaspersky Security Network oraz globalnych statystyk KSN. *Kaspersky Security Network (KSN)* jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobach sieciowych oraz oprogramowaniu. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Endpoint Security na nowe zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. Jeśli uczestniczysz w Kaspersky Security Network, usługi KSN zapewniają Kaspersky Endpoint Security informacje o kategorii i reputacji przeskanowanych plików, a także informacje o reputacji przeskanowanych adresów internetowych.
- **Monitor aktywności aplikacji.** Przeglądaj informacje o działaniu zainstalowanych aplikacji. Kontrola systemu śledzi pliki, rejestr i zdarzenia systemu operacyjnego związane z aplikacją.
- **Monitor sieci.** [Przeglądaj informacje o aktywności komputera](#) w czasie rzeczywistym.

	<ul style="list-style-type: none"> • Monitor szyfrowania. Monitoruje proces szyfrowania lub deszyfrowania dysku w czasie rzeczywistym. Monitor szyfrowania jest dostępny, jeśli komponent Kaspersky Disk Encryption lub komponent Szyfrowanie dysków funkcją BitLocker Drive Encryption jest zainstalowany.
Bezpieczeństwo	Stan działania zainstalowanych komponentów. Możesz także przejść do konfigurowania komponentów lub przeglądania raportów.
Aktualizacja	Zarządzaj zadaniami aktualizacji Kaspersky Endpoint Security. Możesz aktualizować antywirusowe bazy danych i moduły aplikacji oraz wyczościć ostatnią aktualizację . Administrator może ukryć sekcję przed użytkownikiem lub ograniczyć zarządzanie zadaniem .
Zadania	Zarządzaj zadaniami skanowania Kaspersky Endpoint Security. Możesz uruchomić skanowanie antywirusowe i sprawdzenie integralności aplikacji . Administrator może ukrywać zadania przed użytkownikiem lub ograniczyć zarządzanie zadaniami .
Licencja	Licencjonowanie aplikacji. Możesz kupić licencję , aktywować aplikację lub odnowić subskrypcję . Możesz także przejrzeć informacje o bieżącej licencji .
	Konfigurowanie ustawień aplikacji. Administrator może zabronić wprowadzenia zmian w ustawieniach w Kaspersky Security Center .
	Informacje o aplikacji: bieżąca wersja Kaspersky Endpoint Security, data publikacji baz danych, klucz i inne informacje. Możesz przejrzeć zasoby z informacjami firmy Kaspersky, które zawierają przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.
	Wiadomości zawierające informacje o dostępnych aktualizacjach i prośby o dostęp do zaszyfrowanych plików i urządzeń.





Ikona aplikacji w obszarze powiadomień paska zadań

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

Ikona posiada następujące funkcje:

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

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

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

Menu kontekstowe ikony aplikacji zawiera następujące elementy:

- **Kaspersky Endpoint Security for Windows.** Otwiera okno główne aplikacji. W tym oknie możesz dostosować działania składników i zadań aplikacji oraz przejrzeć statystyki przetworzonych plików i wykrytych zagrożeń.

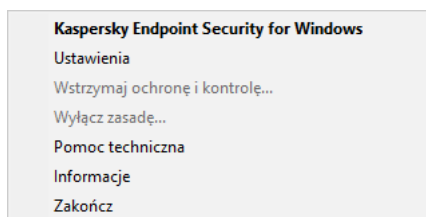
- **Wstrzymaj ochronę / Wznów ochronę.** Wstrzymuje działanie wszystkich składników ochrony i kontroli, które nie są oznaczone kłódką (🔒) w profilu. Przed wykonaniem tego działania, zalecane jest wyłączenie profilu Kaspersky Security Center.

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

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

Wstrzymanie działania składników ochrony i kontroli nie wpływa na działanie zadań aktualizacji i skanowania. Aplikacja będzie też dalej korzystała z Kaspersky Security Network.

- **Wyłącz zasadę / Włącz zasadę.** Wyłącza profil Kaspersky Security Center na komputerze. Wszystkie ustawienia Kaspersky Endpoint Security są dostępne do konfiguracji, włącznie z ustawieniami, które mają zamkniętą kłódkę w profilu (🔒). Jeśli zasada jest wyłączona, aplikacja żąda podania [hasła dostępu do Kaspersky Endpoint Security](#) (hasło do konta lub hasło tymczasowe). Ten element menu kontekstowego jest dostępny, jeśli [ochrona hasłem jest włączona](#). Aby wyłączyć profil, w menu kontekstowym aplikacji wybierz **Włącz zasadę**.
- **Ustawienia.** Otwiera okno ustawień aplikacji.
- **Pomoc techniczna.** To powoduje otwarcie okna zawierającego informacje niezbędne do skontaktowania się z pomocą techniczną Kaspersky.
- **Informacje.** Element ten otwiera okno informacyjne zawierające szczegółowe dane o aplikacji.
- **Zakończ.** Element ten zamyka Kaspersky Endpoint Security. Kliknięcie tego elementu menu kontekstowego powoduje wyładowanie aplikacji z pamięci RAM komputera.



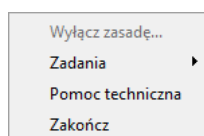
Menu kontekstowe ikony aplikacji

Uproszczony interfejs aplikacji

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

- **Wyłącz zasadę / Włącz zasadę.** Wyłącza profil Kaspersky Security Center na komputerze. Wszystkie ustawienia Kaspersky Endpoint Security są dostępne do konfiguracji, włącznie z ustawieniami, które mają zamkniętą kłódkę w profilu (🔒). Jeśli zasada jest wyłączona, aplikacja żąda podania [hasła dostępu do Kaspersky Endpoint Security](#) (hasło do konta lub hasło tymczasowe). Ten element menu kontekstowego jest dostępny, jeśli [ochrona hasłem jest włączona](#). Aby wyłączyć profil, w menu kontekstowym aplikacji wybierz **Włącz zasadę**.
- **Zadania.** Lista rozwijalna zawierająca następujące elementy:
 - **Sprawdzanie integralności.**

- Wycofywanie baz danych do ich poprzedniej wersji.
- Pełne skanowanie.
- Skanowanie obiektów.
- Skanowanie obszarów krytycznych.
- Aktualizacja.
- **Pomoc techniczna.** To powoduje otwarcie okna zawierającego informacje niezbędne do skontaktowania się z pomocą techniczną Kaspersky.
- **Zakończ.** Element ten zamyka Kaspersky Endpoint Security. Kliknięcie tego elementu menu kontekstowego powoduje wyładowanie aplikacji z pamięci RAM komputera.



Menu kontekstowe ikony aplikacji podczas wyświetlania uproszczonego interfejsu

Konfigurowanie wyświetlania interfejsu aplikacji

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

- **Z uproszczonym interfejsem.** Na komputerze klienckim okno główne aplikacji jest niedostępne, a dostępna jest tylko [ikona w obszarze powiadomień systemu Windows](#). W menu kontekstowym ikony użytkownik może [przeprowadzić ograniczoną liczbę operacji na Kaspersky Endpoint Security](#). Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji.
- **Z pełnym interfejsem.** Na komputerze klienckim dostępne są: okno główne Kaspersky Endpoint Security oraz [ikona w obszarze powiadomień systemu Windows](#). W menu kontekstowym ikony użytkownik może przeprowadzić operacje na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji.
- **Brak interfejsu.** Na komputerze klienckim nie są wyświetlane żadne działania Kaspersky Endpoint Security. [Ikona w obszarze powiadomień systemu Windows](#) oraz powiadomienia nie są dostępne.

[Jak skonfigurować tryb wyświetlania interfejsu aplikacji w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Ustawienia główne** → **Interfejs**.
6. W sekcji **Interakcja z użytkownikiem** wykonaj jedną z następujących czynności:
 - Zaznacz pole **Wyświetl interfejs aplikacji**, jeśli chcesz, żeby na komputerze klienckim były wyświetlane następujące elementy interfejsu:
 - Folder zawierający nazwę aplikacji w menu **Start**
 - [Ikona Kaspersky Endpoint Security](#) w obszarze powiadomień paska zadań systemu Microsoft Windows
 - Powiadomienia wyskakujące

Jeśli to pole jest zaznaczone, użytkownik może przeglądać i, w zależności od dostępnych uprawnień, zmieniać ustawienia aplikacji z poziomu interfejsu aplikacji.

 - Odznacz pole **Wyświetl interfejs aplikacji**, jeśli chcesz ukryć wszystkie oznaki obecności Kaspersky Endpoint Security na komputerze klienckim.
7. W sekcji **Interakcja z użytkownikiem** zaznacz pole **Uproszczony interfejs aplikacji**, jeśli chcesz, żeby [uproszczony interfejs aplikacji](#) był wyświetlany na komputerze klienckim, na którym jest zainstalowany program Kaspersky Endpoint Security.

[Jak skonfigurować tryb wyświetlania interfejsu aplikacji w Web Console i Cloud Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz włączyć obsługę trybu przenośnego.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia główne** → **Interfejs**.
5. W sekcji **Interakcja z użytkownikiem** skonfiguruj sposób wyświetlania interfejsu aplikacji:
 - **Z uproszczonym interfejsem.** Na komputerze klienckim okno główne aplikacji jest niedostępne, a dostępna jest tylko [ikona w obszarze powiadomień systemu Windows](#). W menu kontekstowym ikony użytkownik może [przeprowadzić ograniczoną liczbę operacji na Kaspersky Endpoint Security](#). Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji.
 - **Z pełnym interfejsem.** Na komputerze klienckim dostępne są: okno główne Kaspersky Endpoint Security oraz [ikona w obszarze powiadomień systemu Windows](#). W menu kontekstowym ikony użytkownik może przeprowadzić operacje na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji.
 - **Brak interfejsu.** Na komputerze klienckim nie są wyświetlane żadne działania Kaspersky Endpoint Security. [Ikona w obszarze powiadomień systemu Windows](#) oraz powiadomienia nie są dostępne.
6. Zapisz swoje zmiany.

Rozpoczęcie pracy

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

- Utworzyć i skonfigurować profil.
Istnieje możliwość wykorzystania profili do wprowadzenia identycznych ustawień programu Kaspersky Endpoint Security na wszystkich komputerach klienckich należących do grupy administracyjnej. Kreator wstępnej konfiguracji programu Kaspersky Security Center automatycznie tworzy zasadę dla Kaspersky Endpoint Security.
- Utworzyć zadania *Aktualizacja* i *Skanowanie antywirusowe*.
Zadanie *Aktualizacja* jest wymagane do zapewnienia aktualnej ochrony komputera. Podczas wykonywania zadania Kaspersky Endpoint Security [aktualizuje antywirusowe bazy danych i moduły](#). Zadanie *Aktualizacja* jest tworzone automatycznie przez Kreator wstępnej konfiguracji programu Kaspersky Security Center. Aby utworzyć zadanie *Aktualizacja*, zainstaluj wtyczkę webową Kaspersky Endpoint Security for Windows podczas działania kreatora.
Zadanie *Skanowanie antywirusowe* jest wymagane do natychmiastowego wykrywania wirusów i innych szkodliwych programów. Należy ręcznie utworzyć zadanie *Skanowanie antywirusowe*.

[Jak utworzyć zadanie Skanowanie antywirusowe w Konsoli administracyjnej \(MMC\)?](#) 

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zadania**.

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Nowe zadanie**.

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

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (11.7.0)** → **Skanowanie antywirusowe**.

Krok 2. Obszar skanowania

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

Krok 3. Akcja Kaspersky Endpoint Security

Wybierz akcję po wykryciu zagrożenia:

- **Wylecz; usuń, jeśli leczenie nie jest możliwe.** Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki.
- **Wylecz; poinformuj, jeśli leczenie nie jest możliwe.** Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie nie jest możliwe, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń.
- **Informuj.** Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.
- **Uruchom natychmiast zaawansowane leczenie.** Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security wykorzystuje technologię zaawansowanego leczenia do leczenia aktywnych zagrożeń podczas skanowania.

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

Skonfiguruj tryb uruchamiania zadania za pomocą pola **Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności**. To pole włącza/wyłącza funkcję wstrzymywania zadania *Skanowanie antywirusowe*, gdy zasoby komputera są ograniczone. Kaspersky Endpoint Security wstrzymuje zadanie *Skanowanie antywirusowe*, gdy wygaszacz ekranu jest wyłączony, a komputer jest odblokowany.

Krok 4. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

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

Krok 5. Wybieranie konta do uruchomienia zadania

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

Krok 6. Konfigurowanie terminarza uruchamiania zadania

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

Krok 7. Definiowanie nazwy zadania

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

Krok 8. Kończenie tworzenia zadania

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

[Jak utworzyć zadanie Skanowania antywirusowe w konsoli Web Console?](#) 

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

b. Na liście rozwijanej **Typ zadania** wybierz **Skanowanie antywirusowe**.

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

d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.

5. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

Nowe zadanie zostanie wyświetlone na liście zadań.

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

Zalecane jest skonfigurowanie terminarza uruchamiania zadania przynajmniej raz w tygodniu.

7. Zaznacz pole obok zadania.

8. Kliknij przycisk **Uruchom**.

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

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

Zarządzanie profilami

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

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

Profil aktywny i nieaktywny

Profil jest zarządzany dla grupy zarządzanych komputerów i może być aktywny lub nieaktywny. Ustawienia aktywnego profilu zostaną zapisane na komputerach klienckich podczas synchronizacji. Nie możesz stosować jednocześnie kilku profili na jednym komputerze, dlatego tylko jeden profil może być aktywny w każdej grupie.



Możesz utworzyć nieograniczoną liczbę nieaktywnych profili. Profil nieaktywny nie wpływa na ustawienia aplikacji na komputerach w sieci. Profile nieaktywne są przeznaczone do sytuacji wyjątkowych, takich jak atak wirusa. Jeśli dojdzie do ataku za pośrednictwem dysków flash, możesz aktywować profil, który blokuje dostęp do dysków flash. W tym przypadku profil aktywny automatycznie staje się nieaktywny.

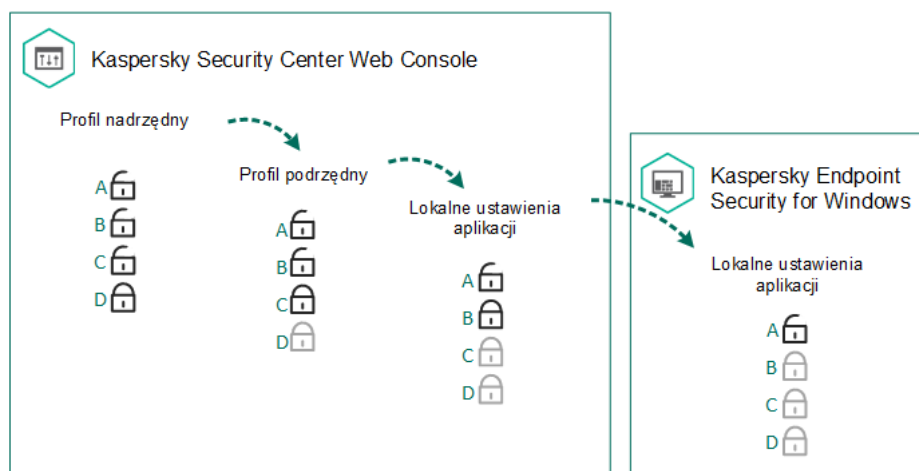
Profil użytkownika mobilnego

Profil użytkownika mobilnego jest aktywowany, gdy komputer opuści sieć obwodową organizacji.

Dziedziczenie ustawień

Zasady, podobnie jak grupy administracyjne, są ułożone w hierarchię. Domyślnie zasada potomna dziedziczy ustawienia z zasady nadrzędnej. *Zasada potomna* to zasada dla zagnieżdżonych poziomów hierarchii, czyli zasada dla zagnieżdżonych grup administracyjnych i podrzędnych Serwerów administracyjnych. Możesz wyłączyć dziedziczenie ustawień z zasady nadrzędnej.

Ustawienia każdej zasady posiadają atrybut , który wskazuje, czy to ustawienie może zostać zmodyfikowane w zasadach potomnych lub w [lokalnych ustawieniach aplikacji](#). Atrybut  jest stosowany tylko wtedy, gdy dziedziczenie ustawień profilu nadrzędnego jest włączone dla profilu potomnego. Profile użytkowników mobilnych nie oddziałują na inne profile poprzez hierarchię grup administracyjnych.



Dziedziczenie ustawień




Uprawnienia dostępu do ustawień profilu (odczyt, zapis, wykonanie) są definiowane dla każdego użytkownika, który posiada dostęp do Serwera administracyjnego Kaspersky Security Center, oraz oddzielnie dla każdego obszaru funkcyjnego Kaspersky Endpoint Security. Aby skonfigurować uprawnienia dostępu do ustawień zasady, przejdź do sekcji **Ochrona** okna właściwości Serwera administracyjnego Kaspersky Security Center.

Tworzenie profilu

[Jak utworzyć zasadę w Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Kliknij przycisk **Nowy profil**.
Zostanie uruchomiony Kreator tworzenia profilu
5. Postępuj zgodnie z instrukcjami Kreatora tworzenia profilu.

[Jak utworzyć zasadę w Web Console i Cloud Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij przycisk **Dodaj**.
Zostanie uruchomiony Kreator tworzenia profilu
3. Wybierz Kaspersky Endpoint Security i kliknij **Dalej**.
4. Przeczytaj i zaakceptuj warunki Oświadczenia Kaspersky Security Network (KSN) i kliknij **Dalej**.
5. Na zakładce **Główne** możesz wykonać następujące działania:
 - Zmień nazwę profilu.
 - Wybierz stan profilu:
 - **Aktywny**. Po kolejnej synchronizacji, profil zostanie użyty jako profil aktywny.
 - **Nieaktywny**. Profil Kopii zapasowej. Jeśli to konieczne, profil nieaktywny może zostać przełączony w stan aktywny.
 - **Profil użytkownika mobilnego**. Profil jest aktywowany, gdy komputer opuści sieć obwodową organizacji.
 - Skonfiguruj dziedziczenie ustawień:
 - **Dziedzicz ustawienia z zasady nadrzędnej**. Jeśli ten przełącznik zostanie ustawiony w pozycji włączenia, wartości ustawień profilu będą dziedziczone z profilu najwyższego poziomu hierarchii. Ustawienia profilu nie mogą być edytowane, jeśli dla profilu nadrzędnego ustawiono .
 - **Wymuś dziedziczenie ustawień w zasadach podrzędnych**. Jeśli przełącznik jest ustawiony w pozycji włączenia, wartości ustawień profilu zostaną przeniesione do profili potomnych. We właściwościach zasady podrzędnej przycisk przełączania **Dziedzicz ustawienia z zasady nadrzędnej** zostanie automatycznie włączony i nie można go wyłączyć. Ustawienia profilu potomnego są dziedziczone z profilu nadrzędnego, za wyjątkiem ustawień oznaczonych . Ustawienia profilu potomnego nie mogą być edytowane, jeśli dla profilu nadrzędnego ustawiono .
6. Na zakładce **Ustawienia aplikacji** możesz skonfigurować [ustawienia profilu Kaspersky Endpoint Security](#).
7. Zapisz swoje zmiany.

W wyniku tego działania ustawienia programu Kaspersky Endpoint Security zostaną skonfigurowane na komputerach klienckich podczas kolejnej synchronizacji. Możesz wyświetlić informacje o zasadzie stosowanej na komputerze w interfejsie Kaspersky Endpoint Security, klikając przycisk **Pomoc techniczna** w oknie głównym (na przykład, nazwę zasady). Aby to zrobić, w ustawieniach zasady Agenta sieciowego należy włączyć odbiór rozszerzonych danych zasad. Więcej informacji na temat zasady Agenta sieciowego można znaleźć w [pomocy do Kaspersky Security Center](#).

Wskaźnik poziomu ochrony

Wskaźnik poziomu ochrony jest wyświetlany w górnej części okna **Właściwości: <nazwa zasady>**. Wskaźnik może przyjąć jedną z następujących wartości:

- **Wysoki poziom ochrony.** Wskaźnik przyjmuje tę wartość oraz kolor zielony, jeśli włączone są wszystkie komponenty z następujących kategorii:
 - **Krytyczne.** Ta kategoria zawiera następujące komponenty:
 - Ochrona plików.
 - Wykrywanie zachowania.
 - Ochrona przed exploitami.
 - Silnik korygujący.
 - **Ważne.** Ta kategoria zawiera następujące komponenty:
 - Kaspersky Security Network.
 - Ochrona WWW.
 - Ochrona poczty.
 - Ochrona przed włamaniami.
- **Średni poziom ochrony.** Wskaźnik przyjmuje tę wartość i staje się żółty, jeśli wyłączony jest jeden z ważnych komponentów.
- **Niski poziom ochrony.** Wskaźnik przyjmuje tę wartość i staje się czerwony w jednej z następujących sytuacji:
 - Wyłączony jest jeden lub kilka krytycznych komponentów.
 - Wyłączony jest jeden lub kilka ważnych komponentów.

Jeśli wskaźnik jest wyświetlany z wartością **Średni poziom ochrony** lub **Niski poziom ochrony**, po prawej stronie wskaźnika pojawi się odnośnik, który otwiera okno **Zalecane składniki ochrony**. W tym oknie możesz włączyć dowolne z zalecanych składników ochrony.

Zarządzanie zadaniami

Możesz utworzyć następujące typy zadań do zarządzania Kaspersky Endpoint Security poprzez Kaspersky Security Center:

- Zadania lokalne konfigurowane dla każdego komputera klienckiego oddzielnie.
- Zadania grupowe konfigurowane dla komputerów klienckich w grupach administracyjnych.
- Zadania dla wyboru komputerów.

Można utworzyć dowolną liczbę zadań grupowych, zadań dla wyborów komputerów oraz zadań lokalnych. Szczegółowe informacje na temat pracy z grupami administracyjnymi i wyborami komputerów *można znaleźć w [pomocy do Kaspersky Security Center](#)*.

Kaspersky Endpoint Security obsługuje następujące zadania:

- **Skanowanie antywirusowe**. Kaspersky Endpoint Security skanuje obszary komputera, określone w ustawieniach zadania, w poszukiwaniu wirusów i innych zagrożeń. Zadanie *Skanowanie antywirusowe* jest wymagane do

działania Kaspersky Endpoint Security i jest tworzone podczas działania Kreatora wstępnej konfiguracji. Zalecane jest [skonfigurowanie terminarza uruchamiania zadania](#) przynajmniej raz w tygodniu.

- **[Dodaj klucz](#)**. Kaspersky Endpoint Security dodaje klucz do aktywowania aplikacji, w tym klucz dodatkowy. Przed uruchomieniem zadania upewnij się, że liczba komputerów, na których zadanie ma zostać wykonane, nie przekracza liczby komputerów dozwolonych przez licencję.
- **[Zmiana składników aplikacji](#)**. Kaspersky Endpoint Security instaluje lub usuwa komponenty na komputerach klienckich zgodnie z listą komponentów określonych w ustawieniach zadania. Moduł Ochrona plików nie może zostać usunięty. Optymalny zestaw komponentów Kaspersky Endpoint Security pomaga oszczędzić zasoby komputera.
- **[Inwentaryzacja](#)**. Kaspersky Endpoint Security zbiera informacje o wszystkich plikach wykonywalnych aplikacji, które są przechowywane na komputerach. Zadanie *Inwentaryzacja* jest wykonywane przez komponent Kontrola aplikacji. Jeśli komponent Kontrola aplikacji nie jest zainstalowany, zadanie zakończy się błędem.
- **[Aktualizacja](#)**. Kaspersky Endpoint Security zaktualizuje bazy danych i moduły aplikacji. Zadanie *Aktualizacja* jest wymagane do działania Kaspersky Endpoint Security i jest tworzone podczas działania Kreatora wstępnej konfiguracji. Zalecane jest skonfigurowanie terminarza, który uruchamia zadanie przynajmniej raz dziennie.
- **[Wyczyść dane](#)**. Kaspersky Endpoint Security usuwa pliki i foldery z komputerów użytkowników od razu lub jeśli nie ma połączenia z Kaspersky Security Center przez dłuższy czas.
- **[Wycofywanie aktualizacji](#)**. Kaspersky Endpoint Security wycofuje ostatnią aktualizację baz danych i modułów aplikacji. Może to być konieczne, jeśli, na przykład, nowe bazy danych zawierają niepoprawne dane, które mogłyby spowodować, że Kaspersky Endpoint Security zablokuje bezpieczną aplikację.
- **[Sprawdzanie integralności](#)**. Kaspersky Endpoint Security analizuje pliki aplikacji, sprawdza pliki pod kątem uszkodzeń i modyfikacji, a także sprawdza podpisy cyfrowe plików aplikacji.
- **[Zarządzanie kontami Agenta autoryzacji](#)**. Kaspersky Endpoint Security konfiguruje ustawienia konta Agenta autoryzacji. Agent autoryzacji jest potrzebny do pracy z zaszyfrowanymi dyskami. Przed załadowaniem systemu operacyjnego użytkownik musi zakończyć uwierzytelnianie za pomocą Agenta.

Zadania są uruchamiane na komputerze tylko wtedy, gdy program [Kaspersky Endpoint Security jest uruchomiony](#).

Dodaj nowe zadanie

[Jak utworzyć zadanie w Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz **Zadania**.
3. Kliknij przycisk **Nowe zadanie**.
Zostanie uruchomiony Kreator tworzenia zadania.
4. Postępuj zgodnie z instrukcjami Kreatora tworzenia zadania.

[Jak utworzyć zadanie w Web Console i Cloud Console?](#)

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

b. Z listy rozwijalnej **Typ zadania** wybierz zadanie, które chcesz uruchomić na komputerach użytkownika.

c. W polu **Nazwa zadania** wpisz krótki opis, na przykład, **Aktualizacja aplikacji dla księgowości**.

d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.

5. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

Nowe zadanie zostanie wyświetlone na liście zadań. Zadanie będzie miało domyślne ustawienia. Aby skonfigurować ustawienia zadania, przejdź do właściwości zadania. Aby uruchomić zadanie, należy zaznaczyć pole obok zadania i kliknąć przycisk **Uruchom**. Po uruchomieniu zadania możesz je zatrzymać i wznowić później.

Na liście zadań możesz monitorować wyniki zadania, które zawierają stan zadania i statystyki wykonania zadania na komputerach. Możesz także utworzyć wybór zdarzeń do monitorowania zakończenia wykonywania zadań (**Monitorowanie i raportowanie** → **Wybory zdarzeń**). Bardziej szczegółowe informacje na temat wyboru zdarzeń można znaleźć w [pomocy do Kaspersky Security Center](#). Wyniki wykonania zadania są także zapisywane lokalnie w dzienniku zdarzeń systemu Windows oraz w [raportach Kaspersky Endpoint Security](#).

Kontrola dostępu do zadań

Uprawnienia dostępu do zadań Kaspersky Endpoint Security (odczyt, zapis, wykonanie) są definiowane dla każdego użytkownika, który posiada dostęp do Serwera administracyjnego Kaspersky Security Center, poprzez ustawienia dostępu do obszarów funkcyjnych Kaspersky Endpoint Security. Aby skonfigurować dostęp do obszarów funkcyjnych Kaspersky Endpoint Security, przejdź do sekcji **Bezpieczeństwo** okna właściwości Serwera administracyjnego Kaspersky Security Center. Więcej informacji na temat zarządzania zadaniami w Kaspersky Security Center można znaleźć w [pomocy dla Kaspersky Security Center](#).

Możesz skonfigurować uprawnienia użytkowników do uzyskiwania dostępu do zadań za pomocą zasady (*tryb zarządzania zadaniami*). Na przykład możesz ukryć zadania grupowe w interfejsie Kaspersky Endpoint Security.

[Jak skonfigurować tryb zarządzania zadaniami w interfejsie Kaspersky Endpoint Security poprzez Konsolę administracyjną \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zadania lokalne** → **Zarządzanie zadaniami**.
6. Skonfiguruj tryb zarządzania zadaniami (patrz tabela poniżej).
7. Zapisz swoje zmiany.

[Jak skonfigurować tryb zarządzania zadaniami w interfejsie Kaspersky Endpoint Security za pośrednictwem Web Console?](#)


1. W oknie głównym Web Console wybierz zakładkę **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz włączyć obsługę trybu przenośnego.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Zadania lokalne** → **Zarządzanie zadaniami**.
5. Skonfiguruj tryb zarządzania zadaniami (patrz tabela poniżej).
6. Zapisz swoje zmiany.

Ustawienia Zarządzania zadaniami

Parametr	Opis
Zezwól na korzystanie z zadań lokalnych	<p>Jeśli pole jest zaznaczone, zadania lokalne są wyświetlane w interfejsie lokalnym Kaspersky Endpoint Security. Jeżeli nie ma dodatkowych ograniczeń profilu, użytkownik może konfigurować i uruchamiać zadania. Jednakże konfigurowanie terminarza uruchamiania zadania pozostaje niedostępne dla użytkownika. Użytkownik może uruchamiać zadania tylko ręcznie.</p> <p>Jeśli pole jest odznaczone, korzystanie z zadań lokalnych zostaje zatrzymane. W tym trybie zadania lokalne nie są uruchamiane zgodnie z terminarzem. Zadania nie mogą być uruchamiane ani konfigurowane w lokalnym interfejsie Kaspersky Endpoint Security lub podczas pracy z wierszem poleceń.</p> <p>Użytkownik może uruchomić skanowanie antywirusowe pliku lub folderu, wybierając opcję Szukaj wirusów w menu kontekstowym pliku lub folderu. Zadanie skanowania jest uruchamiane z domyślnymi wartościami ustawień zadania skanowania obiektów.</p>
Zezwól na wyświetlanie zadań grupowych	<p>Jeśli pole jest zaznaczone, zadania grupowe są wyświetlane w interfejsie lokalnym Kaspersky Endpoint Security. Użytkownik może wyświetlić listę wszystkich zadań w interfejsie aplikacji.</p>

	Jeśli pole nie jest odznaczone, Kaspersky Endpoint Security wyświetla pustą listę zadań.
Zezwól na zarządzanie zadaniami grupowymi	<p>Jeśli to pole jest zaznaczone, użytkownicy mogą uruchamiać i zatrzymywać zadania grupowe określone w Kaspersky Security Center. Użytkownicy mogą uruchamiać i zatrzymywać zadania w interfejsie aplikacji lub w uproszczonym interfejsie aplikacji.</p> <p>Jeśli pole jest odznaczone, Kaspersky Endpoint Security automatycznie uruchamia zaplanowane zadania lub administrator uruchamia zadania ręcznie w Kaspersky Security Center.</p>

Konfigurowanie lokalnych ustawień aplikacji

W Kaspersky Security Center możesz skonfigurować ustawienia Kaspersky Endpoint Security na określonym komputerze. Są to *lokalne ustawienia aplikacji*. Niektóre ustawienia mogą być niedostępne do edycji. Te ustawienia są zablokowane przez atrybut  we [właściwościach profilu](#).

[Jak skonfigurować lokalne ustawienia aplikacji w Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, do której należy wybrany komputer kliencki.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Wybierz komputer, dla którego chcesz skonfigurować ustawienia Kaspersky Endpoint Security.
5. Z otwartego menu kontekstowego komputera klienckiego wybierz **Właściwości**.
Zostanie otwarte okno właściwości komputera klienckiego.
6. W oknie ustawień komputera wybierz sekcję **Aplikacje**.
Lista aplikacji Kaspersky, które są zainstalowane na komputerze klienckim, pojawi się w prawej części okna właściwości komputera klienckiego.
7. Zaznacz Kaspersky Endpoint Security.
8. Kliknij przycisk **Właściwości** pod listą aplikacji firmy Kaspersky.
To spowoduje otwarcie okna **Ustawienia aplikacji Kaspersky Endpoint Security for Windows**.
9. W sekcji **Ustawienia główne** skonfiguruj Kaspersky Endpoint Security, a także Raporty i pliki danych.
Pozostałe sekcje okna **Ustawienia aplikacji Kaspersky Endpoint Security for Windows** są takie same jak standardowe sekcje aplikacji Kaspersky Security Center. Opis tych sekcji można znaleźć w systemie pomocy programu Kaspersky Security Center.

Jeśli aplikacja podlega profilowi, który blokuje wprowadzanie zmian w określonych ustawieniach, nie będziesz mógł ich zmodyfikować w trakcie konfiguracji ustawień aplikacji w sekcji **Ustawienia główne**.

10. W celu zapisania zmian, wprowadzonych w oknie **Ustawienia aplikacji Kaspersky Endpoint Security for Windows**, kliknij **OK**.

Jak skonfigurować lokalne ustawienia aplikacji w konsoli Web Console i Cloud Console?

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.
Spowoduje to otwarcie właściwości komputera.
3. Wybierz zakładkę **Aplikacje**.
4. Kliknij **Kaspersky Endpoint Security for Windows**.
Spowoduje to otwarcie lokalnych ustawień aplikacji.
5. Wybierz zakładkę **Ustawienia aplikacji**.
6. Skonfiguruj lokalne ustawienia aplikacji.
7. Lokalne ustawienia aplikacji są takie same, jak [ustawienia profilu](#), za wyjątkiem ustawień szyfrowania.

Uruchamianie i zatrzymywanie Kaspersky Endpoint Security

Po zainstalowaniu Kaspersky Endpoint Security na komputerze użytkownika, aplikacja jest uruchamiana automatycznie. Domyślnie, Kaspersky Endpoint Security jest uruchamiany po załadowaniu systemu operacyjnego. Nie można skonfigurować automatycznego uruchamiania aplikacji w ustawieniach systemu operacyjnego.

Pobieranie antywirusowych baz danych Kaspersky Endpoint Security po uruchomieniu systemu operacyjnego może zająć do dwóch minut w zależności od możliwości komputera. W tym czasie poziom ochrony zostanie zredukowany. Pobieranie antywirusowych baz danych, gdy Kaspersky Endpoint Security jest uruchomiony na już załadowanym systemie operacyjnym, nie spowoduje zredukowania poziomu ochrony komputera.


Jak skonfigurować uruchamianie Kaspersky Endpoint Security w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Ustawienia ogólne** → **Zarządzanie zadaniami**.
6. Użyj pola **Włącz Kaspersky Endpoint Security for Windows podczas uruchamiania komputera**, aby skonfigurować uruchamianie aplikacji.
7. Zapisz swoje zmiany.

Jak skonfigurować uruchamianie Kaspersky Endpoint Security w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę profilu Kaspersky Endpoint Security dla komputerów, dla których chcesz skonfigurować uruchamianie aplikacji.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia główne**.
5. Kliknij odnośnik **Ustawienia aplikacji**.
6. Użyj pola **Włącz Kaspersky Endpoint Security for Windows** podczas uruchamiania komputera, aby skonfigurować uruchamianie aplikacji.
7. Zapisz swoje zmiany.



Jak skonfigurować uruchamianie Kaspersky Endpoint Security w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia aplikacji**.
3. Użyj pola **Włącz Kaspersky Endpoint Security for Windows** podczas uruchamiania komputera, aby skonfigurować uruchamianie aplikacji.
4. Zapisz swoje zmiany.

Ekspersi z Kaspersky nie zalecają ręcznego wyłączenia Kaspersky Endpoint Security, ponieważ narazi to komputer i dane osobowe na zagrożenia. W razie konieczności możesz [wstrzymać ochronę komputera](#) na tak długo jak potrzebujesz, bez wyłączania aplikacji.

Możesz monitorować stan aplikacji za pomocą widżetu **Stan ochrony**.

Jak uruchomić lub zatrzymać Kaspersky Endpoint Security w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, do której należy wybrany komputer kliencki.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Wybierz komputer, na którym chcesz uruchomić lub zatrzymać aplikację.
5. Kliknij prawym przyciskiem myszy komputer kliencki, aby wyświetlić jego menu kontekstowe, z którego wybierz **Właściwości**.
6. W oknie ustawień komputera wybierz sekcję **Aplikacje**.
Lista aplikacji Kaspersky, które są zainstalowane na komputerze klienckim, pojawi się w prawej części okna właściwości komputera klienckiego.
7. Zaznacz Kaspersky Endpoint Security.
8. Wykonaj następujące czynności:
 - W celu uruchomienia aplikacji kliknij przycisk  na prawo od listy aplikacji Kaspersky.
 - W celu zatrzymania aplikacji kliknij przycisk  na prawo od listy aplikacji Kaspersky.

[Jak uruchomić lub zatrzymać Kaspersky Endpoint Security w konsoli Web Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Kliknij nazwę tego komputera, na którym chcesz uruchomić lub zatrzymać działanie Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości komputera.
3. Wybierz zakładkę **Aplikacje**.
4. Zaznacz pole obok **Kaspersky Endpoint Security for Windows**.
5. Kliknij przycisk **Uruchom** lub **Zatrzymaj**.

[Jak uruchomić lub zatrzymać Kaspersky Endpoint Security z poziomu wiersza poleceń?](#)

Aby zatrzymać aplikację z poziomu wiersza poleceń, [włącz możliwość zewnętrznego zarządzania usługami systemowymi](#).



Plik klpsm.exe, który znajduje się w pakiecie dystrybucyjnym Kaspersky Endpoint Security, jest używany do uruchamiania lub zatrzymywania aplikacji z poziomu wiersza poleceń.

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.
3. Aby uruchomić aplikację z poziomu wiersza polecenia, wpisz `klpsm.exe start_avp_service`.
4. Aby zatrzymać aplikację z poziomu wiersza polecenia, wpisz `klpsm.exe stop_avp_service`.

Wstrzymywanie i wznowianie kontroli i ochrony komputera

Pojęcie wstrzymywania kontroli i ochrony komputera oznacza wyłączenie na pewien czas wszystkich składników kontroli i ochrony programu Kaspersky Endpoint Security.

Stan aplikacji jest wyświetlany przy pomocy [ikony aplikacji w obszarze powiadomień paska zadań](#).

- Ikona  oznacza, że kontrola i ochrona komputera zostały wstrzymane.
- Ikona  oznacza, że kontrola i ochrona komputera zostały włączone.

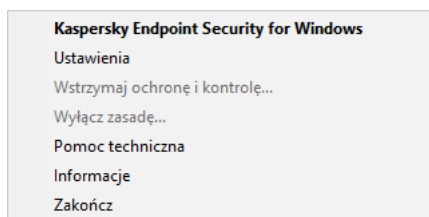
Wstrzymywanie lub wznowianie kontroli i ochrony komputera nie ma wpływu na zadania skanowania i aktualizacji.

Jeżeli podczas wstrzymywania lub wznowiania kontroli i ochrony komputera nawiązane są jakiegokolwiek połączenia sieciowe, wówczas zostanie wyświetlone powiadomienie o zerwaniu tych połączeń.

W celu wstrzymania kontroli i ochrony komputera:

1. Kliknij prawym przyciskiem myszy ikonę aplikacji znajdującą się w obszarze powiadomień paska zadań.
2. Z otwartego menu kontekstowego wybierz **Wstrzymaj ochronę** (patrz rysunek poniżej).
Ten element menu kontekstowego jest dostępny, jeśli [ochrona hasłem jest włączona](#).
3. Wybierz jedną z następujących opcji:
 - **Wstrzymaj na <określony czas>** – kontrola i ochrona komputera zostaną wznowione po upływie czasu wybranego z listy rozwijalnej dostępnej poniżej.
 - **Wstrzymaj do restartu aplikacji** – kontrola i ochrona komputera zostaną wznowione po ponownym uruchomieniu aplikacji lub systemu operacyjnego. Aby użyć tej opcji, należy włączyć automatyczne uruchamianie aplikacji.
 - **Wstrzymaj** – kontrola i ochrona komputera zostaną wznowione na Twoje żądanie.
4. Kliknij przycisk **Wstrzymaj ochronę**.

Kaspersky Endpoint Security wstrzymuje działanie wszystkich składników ochrony i kontroli, które nie są oznaczone kłódką (🔒) w profilu. Przed wykonaniem tego działania, zalecane jest wyłączenie profilu Kaspersky Security Center.



Menu kontekstowe ikony aplikacji

W celu wznowienia kontroli i ochrony komputera:

1. Kliknij prawym przyciskiem myszy ikonę aplikacji znajdującą się w obszarze powiadomień paska zadań.
2. Z otwartego menu kontekstowego wybierz **Wznów ochronę**.

Możesz wznowić kontrolę i ochronę komputera w dowolnym momencie, niezależnie od wybranej opcji wstrzymania kontroli i ochrony komputera.

Skanowanie antywirusowe komputera

Skonowanie antywirusowe jest niezwykle ważne dla bezpieczeństwa komputera. Regularne uruchamianie skanowania antywirusowego pozwala wyeliminować możliwość rozpowszechniania się szkodliwego oprogramowania, które nie jest wykrywane przez moduły ochrony z powodu ustawienia niskiego poziomu ochrony lub z innych powodów.

Kaspersky Endpoint Security nie skanuje plików, których zawartość znajduje się w magazynie w chmurze OneDrive, i tworzy wpisy dziennika informujące, że pliki te nie zostały przeskanowane.

Pełne skanowanie

Szczegółowe skanowanie całego komputera. Kaspersky Endpoint Security skanuje następujące obiekty:

- Pamięć jądra
- Obiekty uruchamiane wraz ze startem systemu operacyjnego
- Sektory startowe.
- Kopię zapasową systemu operacyjnego
- Wszystkie dyski twarde i wymienne.

Ekspert z Kaspersky zalecają, aby nie zmieniać obszaru skanowania zadania *Pełnego skanowania*.

Aby zachować zasoby komputera, zalecane jest użycie [zadania skanowania w tle](#) zamiast zadania pełnego skanowania. Nie wpłynie to na poziom ochrony komputera.

Skonowanie obszarów krytycznych

Domyślnie, Kaspersky Endpoint Security skanuje pamięć jądra, uruchomione procesy i sektory startowe dysku.

Ekspert z Kaspersky zalecają, aby nie zmieniać obszaru skanowania zadania *Skonowania obszarów krytycznych*.

Skonowanie obiektów

Kaspersky Endpoint Security skanuje obiekty wybrane przez użytkownika. Możesz skanować każdy obiekt z poniższej listy:

- Pamięć systemowa
- Obiekty uruchamiane wraz ze startem systemu operacyjnego
- Kopię zapasową systemu operacyjnego

- Skanuje skrzynkę pocztową programu Microsoft Outlook
- Dyski twarde, wymienne i sieciowe
- Dowolny wybrany plik

Skanowanie w tle

Skanowanie w tle to tryb skanowania programu Kaspersky Endpoint Security, który nie wyświetla powiadomień. Skanowanie w tle wymaga mniej zasobów komputera niż inne typy skanowań (takie jak pełne skanowanie). W tym trybie Kaspersky Endpoint Security skanuje obiekty startowe, sektory startowe, pamięć systemową i partycje systemowe.

Sprawdzanie integralności

Kaspersky Endpoint Security sprawdza, czy moduły aplikacji nie są uszkodzone lub zmodyfikowane.

Skanowanie komputera

Skanowanie antywirusowe jest niezwykle ważne dla bezpieczeństwa komputera. Regularne uruchamianie skanowania antywirusowego pozwala wyeliminować możliwość rozpowszechniania się szkodliwego oprogramowania, które nie jest wykrywane przez moduły ochrony z powodu ustawienia niskiego poziomu ochrony lub z innych powodów. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, [usługi w chmurze Kaspersky Security Network](#) i analizy heurystycznej.

Kaspersky Endpoint Security zawiera standardowe, predefiniowane zadania: *Pełne skanowanie*, *Skanowanie obszarów krytycznych*, *Skanowanie obiektów*. Jeśli w Twojej organizacji wdrożono system administracyjny Kaspersky Security Center, możesz [utworzyć zadanie *Skanowania antywirusowego*](#) i skonfigurować skanowanie. Zadanie [Skanowanie w tle](#) jest dostępne także w Kaspersky Security Center. Skanowania w tle nie można skonfigurować.

[Jak w Konsoli administracyjnej \(MMC\) uruchomić Skanowanie antywirusowe?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zadania**.
4. Wybierz zadanie skanowania i kliknij je dwukrotnie, aby otworzyć właściwości zadania.
Jeśli to konieczne, [utwórz zadanie Skanowanie antywirusowe](#).
5. W oknie właściwości zadania wybierz sekcję **Ustawienia**.
6. Skonfiguruj zadanie skanowanie (patrz tabela poniżej).
Jeśli to konieczne, [skonfiguruj terminarz zadania skanowania](#).
7. Zapisz swoje zmiany.
8. Uruchom zadanie skanowania.


Kaspersky Endpoint Security uruchomi skanowanie komputera. Jeśli użytkownik przerwał wykonywanie zadania (na przykład, poprzez wyłączenie komputera), Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane.

[Jak w konsoli Web Console i Cloud Console uruchomić Skanowanie antywirusowe?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Kliknij zadanie skanowania.
Zostanie otwarte okno właściwości zadania.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Skonfiguruj zadanie skanowanie (patrz tabela poniżej).
Jeśli to konieczne, [skonfiguruj terminarz zadania skanowania](#).
5. Zapisz swoje zmiany.
6. Uruchom zadanie skanowania.

Kaspersky Endpoint Security uruchomi skanowanie komputera. Jeśli użytkownik przerwał wykonywanie zadania (na przykład, poprzez wyłączenie komputera), Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane.

[Jak w interfejsie aplikacji uruchomić Skanowanie antywirusowe?](#)



1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij .
3. Skonfiguruj zadanie skanowanie (patrz tabela poniżej).
Jeśli to konieczne, [skonfiguruj terminarz zadania skanowania](#).
4. Zapisz swoje zmiany.
5. Uruchom zadanie skanowania.

Kaspersky Endpoint Security uruchomi skanowanie komputera. Aplikacja wyświetli postęp skanowania, liczbę przeskanowanych plików oraz czas pozostały do skanowania. Kliknij przycisk **Zatrzymaj**, aby zatrzymać zadanie w dowolnym momencie. Jeśli zadanie skanowania nie jest wyświetlane, oznacza to, że administrator [zabronił użycia zadań lokalnych w zasadzie](#).

Ustawienia skanowania

Parametr	Opis
Poziom ochrony	<p>Kaspersky Endpoint Security może używać różnych grup ustawień uruchamiania skanowania. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane <i>poziomami ochrony</i>.</p> <ul style="list-style-type: none"> • Wysoki. Kaspersky Endpoint Security skanuje wszystkie typy plików. Podczas skanowania plików złożonych Kaspersky Endpoint Security skanuje również pliki w formatach pocztowych. • Zalecany. Kaspersky Endpoint Security skanuje tylko określone formaty plików na wszystkich dyskach twardych, dyskach sieciowych i wymiennych nośnikach danych oraz wbudowane obiekty OLE. Kaspersky Endpoint Security nie skanuje archiwów ani pakietów instalacyjnych. • Niski. Kaspersky Endpoint Security skanuje tylko nowe lub zmodyfikowane pliki o określonych rozszerzeniach na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Kaspersky Endpoint Security nie skanuje plików złożonych. <p>Możesz wybrać jeden z predefiniowanych poziomów ochrony lub ręcznie skonfigurować ustawienia poziomu ochrony. Jeśli zmienisz ustawienia poziomu ochrony, możesz zawsze powrócić do zalecanych ustawień poziomu ochrony.</p>
Działanie podejmowane w przypadku wykrycia zagrożenia	<p>Wylecz; usuń, jeśli leczenie nie jest możliwe. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki.</p> <p>Wylecz; poinformuj, jeśli leczenie nie jest możliwe. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie nie jest możliwe, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń.</p> <p>Informuj. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.</p>

	<p>Przed próbą wyleczenia lub usunięcia zainfekowanego pliku, Kaspersky Endpoint Security utworzy kopię zapasową pliku w przypadku, gdy potrzebujesz przywrócić plik lub jeśli może zostać wyleczony w przyszłości.</p>
	<p>Po wykryciu zainfekowanych plików, które są częścią aplikacji Sklep Windows, Kaspersky Endpoint Security spróbuje usunąć plik.</p>
<p>Uruchom natychmiast Zaawansowane leczenie</p> <p><i>(dostępny tylko w Kaspersky Security Center Console)</i></p>	<p>Zaawansowane leczenie podczas wykonywania zadania skanowania antywirusowego na komputerze jest wykonywane tylko wtedy, gdy funkcja Zaawansowane leczenie jest włączona we właściwościach zasady zastosowanej do tego komputera.</p> <p>Jeśli pole zostało zaznaczone, Kaspersky Endpoint Security wyleczy aktywną infekcję od razu po jej wykryciu podczas wykonywania zadania skanowania antywirusowego. Po wyleczeniu aktywnej infekcji, Kaspersky Endpoint Security uruchamia komputer ponownie bez pytania użytkownika.</p> <p>Jeśli pole zostało odznaczone, Kaspersky Endpoint Security nie wyleczy aktywnej infekcji od razu po jej wykryciu podczas wykonywania zadania skanowania antywirusowego. Kaspersky Endpoint Security generuje zdarzenia aktywnej infekcji w lokalnych raportach aplikacji i po stronie Kaspersky Security Center. Aktywna infekcja może zostać wyleczona, gdy zadanie skanowania antywirusowego jest uruchamiane z włączoną funkcją Zaawansowanego leczenia. W ten sposób administrator systemu może wybrać odpowiedni czas na przeprowadzenie Zaawansowanego leczenia i następnie automatyczne ponowne uruchomienie komputera.</p>
<p>Obszar skanowania</p>	<p>Lista obiektów, które są skanowane przez Kaspersky Endpoint Security podczas wykonywania zadania skanowania. Obiekty z obszaru skanowania mogą zawierać pamięć jądra, uruchomione procesy, sektory startowe, miejsce przechowywania kopii zapasowej systemu, pocztowe bazy danych, dyski twarde lub sieciowe, nośniki wymienne, foldery lub pliki.</p>
<p>Terminarz skanowania</p>	<p>Ręcznie. Tryb uruchamiania, w którym możesz ręcznie uruchomić skanowanie w wygodnym dla siebie momencie.</p> <p>Zgodnie z terminarzem. W tym trybie Kaspersky Endpoint Security uruchamia zadanie skanowania zgodnie z ustalonym terminarzem. Jeśli wybrano ten tryb uruchamiania, zadanie skanowania może również zostać uruchomione ręcznie.</p>
<p>Uruchom po N minutach od uruchomienia aplikacji</p>	<p>Odroczone uruchomienie zadania skanowania po uruchomieniu aplikacji. Przy uruchamianiu systemu operacyjnego wiele procesów jest uruchomionych, dlatego korzystne jest odroczenie uruchomienia zadania skanowania zamiast uruchomienie do od razu po uruchomieniu Kaspersky Endpoint Security.</p>
<p>Uruchom pominięte zadania</p>	<p>Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security uruchamia pominięte zadanie skanowania, kiedy tylko będzie to możliwe. Zadanie skanowania może zostać pominięte, na przykład, jeśli komputer był wyłączony w zaplanowanym czasie uruchomienia zadania skanowania. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie uruchamia pominiętych zadań skanowania. Zamiast tego uruchomi następnne zadanie skanowania zgodnie z bieżącym terminarzem.</p>
<p>Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności</p>	<p>Odroczono uruchomienie zadania skanowania, gdy zasoby komputera są zajęte. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałes wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane.</p>

<p>Uruchom skanowanie jako</p>	<p>Domyślnie zadanie skanowania jest uruchamiane w imieniu użytkownika, z którego uprawnieniami jesteś zarejestrowany w systemie operacyjnym. Obszar ochrony może zawierać dyski sieciowe lub inne obiekty, które wymagają specjalnych uprawnień dostępu. Możesz wskazać użytkownika, który posiada odpowiednie uprawnienia, w ustawieniach Kaspersky Endpoint Security i uruchomić skanowanie z poziomu konta tego użytkownika.</p>
<p>Typy plików</p>	<div data-bbox="395 327 1493 486" style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>Program Kaspersky Endpoint Security traktuje pliki bez rozszerzeń jak pliki wykonywalne. Kaspersky Endpoint Security zawsze skanuje pliki wykonywalne bez względu na typy plików wybrane do skanowania.</p> </div> <p>Wszystkie pliki. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia).</p> <p>Pliki skanowane według formatu. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował tylko infekowalne pliki . Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików.</p> <p>Pliki skanowane według rozszerzenia. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował tylko infekowalne pliki . Format pliku będzie określany w oparciu o jego rozszerzenie.</p> <p>Domyślnie program Kaspersky Endpoint Security skanuje pliki według ich formatu. Skanowanie plików według rozszerzenia jest mniej bezpieczne, ponieważ szkodliwy plik może mieć rozszerzenie, które nie znajduje się na liście potencjalnie infekowalnych (na przykład: .123).</p>
<p>Skanuj tylko nowe i zmienione pliki</p>	<p>Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.</p>
<p>Pomiń pliki skanowane dłużej niż N s</p>	<p>Ogranicza czas skanowania pojedynczego obiektu. Po określonym czasie Kaspersky Endpoint Security przestanie skanować plik. To pomaga skrócić czas skanowania.</p>
<p>Skanuj archiwa</p>	<p>Skanuje archiwa w następujących formatach: RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.</p>
<p>Skanuj pakiety dystrybucyjne</p>	<p>To pole włącza/wyłącza skanowanie pakietów dystrybucyjnych firm trzecich.</p>
<p>Skanuj pliki w formatach Microsoft Office</p>	<p>Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty.</p>
<p>Skanuj formaty poczty elektronicznej</p>	<p>Ta opcja włącza / wyłącza dla Kaspersky Endpoint Security opcję skanowania plików w formatach pocztowych i bazach danych poczty.</p> <p>Aplikacja całkowicie skanuje tylko formaty plików MS Outlook, Windows Mail/Outlook Express i EML i tylko wtedy, gdy na komputerze znajduje się klient poczty MS Outlook x86.</p> <p>Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security rozkłada pliki w formatach pocztowych na składniki (nagłówki, ciało, załączniki) i skanuje je w poszukiwaniu zagrożeń.</p> <p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki w formatach pocztowych jako pojedyncze pliki.</p>
<p>Skanuj archiwa zabezpieczone hasłem</p>	<p>Jeżeli pole jest zaznaczone, Kaspersky Endpoint Security skanuje archiwa zabezpieczone hasłem. Zanim pliki w archiwum zostaną przeskanowane, zostaniesz poproszony o wpisanie hasła.</p>

	<p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security pomija skanowanie archiwów chronionych hasłem.</p>
<p>Nie rozpakowuj dużych plików złożonych</p>	<p>Jeżeli to pole jest zaznaczone, Kaspersky Endpoint Security nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość.</p> <p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki złożone o wszystkich rozmiarach.</p> <p>Kaspersky Endpoint Security skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.</p>
<p>Uczenie maszynowe i analiza sygnatur</p>	<p>Metoda uczenia maszynowego i analiza sygnatur używa baz danych Kaspersky Endpoint Security, które zawierają opisy znanych zagrożeń oraz metody ich neutralizowania. Ochrona korzystająca z tej metody zapewnia minimalny dopuszczalny poziom ochrony.</p> <p>W oparciu o zalecenia ekspertów z Kaspersky, uczenie maszynowe i analiza sygnatur jest zawsze włączona.</p>
<p>Analiza heurystyczna</p>	<p>Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa.</p> <p>Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.</p>
<p>Technologia iSwift</p> <p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.</p>
<p>Technologia iChecker</p> <p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).</p>

Skanowanie napędów wymiennych po ich podłączeniu do komputera

Kaspersky Endpoint Security skanuje wszystkie pliki, które uruchamiasz lub kopiujesz nawet wtedy, gdy plik znajduje się na dysku wymiennym (komponent Ochrona plików). Aby zapobiec rozprzestrzenianiu wirusów i innych szkodliwych programów, możesz skonfigurować automatyczne skanowania dysków wymiennych po ich podłączeniu do komputera. Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki. Komponent zapewnia ochronę komputera poprzez wykonywanie skanowań, które implementują uczenie maszynowe, analizę heurystyczną (wysoki poziom) oraz analizę przy użyciu sygnatur. Kaspersky Endpoint Security używa także technologii optymalizacji skanowania iSwift i iChecker. Technologie są zawsze włączone i nie mogą zostać wyłączone.


[Jak w Konsoli administracyjnej \(MMC\) skonfigurować uruchamianie Skanowania dysków wymiennych?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zadania lokalne** → **Skanowanie dysków wymiennych**.
6. Z listy rozwijalnej **Akcja po podłączeniu dysku wymiennego** wybierz **Skanowanie szczegółowe** lub **Szybkie skanowanie**.
7. Skonfiguruj zaawansowane opcje Skanowania dysków wymiennych (patrz tabela poniżej).
8. Zapisz swoje zmiany.

[Jak w konsoli Web Console i Cloud Console skonfigurować uruchamianie Skanowania dysków wymiennych?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Zadania lokalne** → **Skanowanie dysków wymiennych**.
5. Z listy rozwijalnej **Akcja po podłączeniu dysku wymiennego** wybierz **Skanowanie szczegółowe** lub **Szybkie skanowanie**.
6. Skonfiguruj zaawansowane opcje Skanowania dysków wymiennych (patrz tabela poniżej).
7. Zapisz swoje zmiany.

[Jak w interfejsie aplikacji skonfigurować uruchamianie Skanowania dysków wymiennych?](#)

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij .
3. Użyj przełącznika **Skanowanie dysków wymiennych**, aby włączyć lub wyłączyć skanowanie nośników wymiennych po podłączeniu do komputera.
4. Skonfiguruj zaawansowane opcje Skanowania dysków wymiennych (patrz tabela poniżej).
5. Zapisz swoje zmiany.

W wyniku tego działania Kaspersky Endpoint Security uruchomi Skanowanie dysków wymiennych dla dysków wymiennych, które nie są większe niż określony maksymalny rozmiar. Jeśli zadanie *Skanowanie dysków wymiennych* nie jest wyświetlane, to oznacza, że administrator [zabronił używania zadań lokalnych w zasadzie](#).

Ustawienia zadania Skanowanie dysków wymiennych

Parametr	Opis
Akcja po podłączeniu dysku wymiennego	<p>Skanowanie szczegółowe Jeśli ten element został wybrany, po podłączeniu dysku wymiennego, Kaspersky Endpoint Security skanuje wszystkie pliki na dysku wymiennym, w tym pliki zagnieżdżone w obiektach złożonych, archiwach, pakietach dystrybucyjnych oraz plikach w formatach office. Kaspersky Endpoint Security nie skanuje plików w formatach pocztowych ani archiwach chronionych hasłem.</p> <p>Szybkie skanowanie Jeśli ta opcja jest zaznaczona, po podłączeniu dysku wymiennego, Kaspersky Endpoint Security skanuje tylko pliki określonych formatów, które są najbardziej podatne na infekcje, i nie rozpakowuje obiektów złożonych.</p>
Maksymalny rozmiar dysku wymiennego	<p>Jeżeli pole jest zaznaczone, Kaspersky Endpoint Security wykona na nośnikach wymiennych, których rozmiar nie przekracza zdefiniowanej wartości, akcję wybraną z listy rozwijalnej Akcja po podłączeniu dysku wymiennego.</p> <p>Jeżeli pole nie jest zaznaczone, Kaspersky Endpoint Security wykona na nośnikach wymiennych o dowolnym rozmiarze akcję wybraną z listy rozwijalnej Akcja po podłączeniu dysku wymiennego.</p>
Pokaż postęp skanowania	<p>Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security wyświetli postęp skanowania nośników wymiennych w oddzielnym oknie oraz w oknie Zadania.</p> <p>Jeśli pole jest odznaczone, Kaspersky Endpoint Security uruchomi skanowanie nośników wymiennych w tle.</p>
Blokuj zatrzymywanie zadania skanowania	<p>Jeśli pole jest zaznaczone, przycisk Zatrzymaj w oknie Zadania oraz przycisk Zatrzymaj w oknie Skanowanie antywirusowe są niedostępne w interfejsie lokalnym Kaspersky Endpoint Security.</p>

Skanowanie w tle

Skanowanie w tle to tryb skanowania programu Kaspersky Endpoint Security, który nie wyświetla powiadomień. Skanowanie w tle wymaga mniej zasobów komputera niż inne typy skanowań (takie jak pełne skanowanie). W tym trybie Kaspersky Endpoint Security skanuje obiekty startowe, sektory startowe, pamięć systemową i partycje systemowe. Skanowanie w tle jest uruchamiane w następujących przypadkach:

- Po aktualizacji antywirusowych baz danych.

- 30 minut po uruchomieniu Kaspersky Endpoint Security.
- Co sześć godzin.
- Gdy komputer jest w stanie bezczynności przez pięć minut lub dłużej (komputer jest zablokowany lub włączony jest wygaszacz ekranu).

Skanowanie w tle, gdy komputer jest w stanie bezczynności, zostaje przerwane, gdy którykolwiek z poniższych warunków jest prawdziwy:

- Komputer działa w trybie aktywnym.

Jeśli skanowanie w tle nie było wykonywane dłużej niż dziesięć dni temu, skanowanie nie jest przerywane.

- Komputer (laptop) przełączył się w tryb pracy na bateriach.

Jeśli uruchamiasz zadanie skanowania w tle, Kaspersky Endpoint Security nie skanuje plików, których zawartość znajduje się w magazynie w chmurze OneDrive.


[Jak w Konsoli administracyjnej \(MMC\) włączyć skanowanie w tle?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zadania lokalne** → **Skanowanie w tle**.
6. Użyj pola **Skanowanie w tle**, aby włączyć lub wyłączyć skanowanie w tle.
7. Zapisz swoje zmiany.

[Jak w konsoli Web Console i Cloud Console włączyć skanowanie w tle?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Zadania lokalne** → **Skanowanie w tle**.
5. Użyj pola **Skanowanie w tle**, aby włączyć lub wyłączyć skanowanie w tle.
6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji włączyć skanowanie w tle?

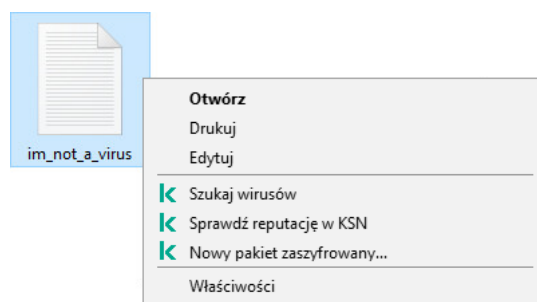
1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij .
3. Użyj przełącznika **Skanowanie w tle**, aby włączyć lub wyłączyć skanowanie w tle.
4. Zapisz swoje zmiany.

Jeśli *Skanowanie w tle* nie jest wyświetlane, to oznacza, że administrator [zabronił używania zadań lokalnych w zasadzie](#).

Skanowanie z menu kontekstowego

Kaspersky Endpoint Security umożliwia uruchomienie skanowania pojedynczych plików w poszukiwaniu wirusów i innych szkodliwych programów z poziomu menu kontekstowego (patrz rysunek poniżej).

Jeśli uruchamiasz skanowanie z poziomu menu kontekstowego, Kaspersky Endpoint Security nie skanuje plików, których zawartość znajduje się w magazynie w chmurze OneDrive.



Skanowanie z menu kontekstowego


Jak w Konsoli administracyjnej (MMC) skonfigurować Skanowanie z menu kontekstowego?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zadania lokalne** → **Skanowanie z menu kontekstowego**.
6. Skonfiguruj Skanowanie z menu kontekstowego (patrz tabela poniżej).
7. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console skonfigurować Skanowanie z menu kontekstowego?

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Zadania lokalne** → **Skanowanie z menu kontekstowego**.
5. Skonfiguruj Skanowanie z menu kontekstowego (patrz tabela poniżej).
6. Zapisz swoje zmiany.



Jak w interfejsie aplikacji skonfigurować Skanowanie z menu kontekstowego?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij .
3. Skonfiguruj Skanowanie z menu kontekstowego (patrz tabela poniżej).
4. Zapisz swoje zmiany.

Jeśli zadanie *Skanowanie z menu kontekstowego* nie zostało wyświetlone, to oznacza, że administrator [zabronił używania zadań lokalnych w zasadzie](#).

Ustawienia zadania Skanowanie z menu kontekstowego

Parametr	Opis
Poziom ochrony	Kaspersky Endpoint Security może używać różnych grup ustawień uruchamiania skanowania. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane <i>poziomami ochrony</i> .

	<ul style="list-style-type: none"> • Wysoki. Kaspersky Endpoint Security skanuje wszystkie typy plików. Podczas skanowania plików złożonych Kaspersky Endpoint Security skanuje również pliki w formatach pocztowych. • Zalecany. Kaspersky Endpoint Security skanuje tylko określone formaty plików na wszystkich dyskach twardych, dyskach sieciowych i wymiennych nośnikach danych oraz wbudowane obiekty OLE. Kaspersky Endpoint Security nie skanuje archiwów ani pakietów instalacyjnych. • Niski. Kaspersky Endpoint Security skanuje tylko nowe lub zmodyfikowane pliki o określonych rozszerzeniach na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Kaspersky Endpoint Security nie skanuje plików złożonych.
Działanie podejmowane w przypadku wykrycia zagrożenia	<p>Wylecz; usuń, jeśli leczenie nie jest możliwe. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki.</p> <p>Wylecz; blokuj, jeśli leczenie nie jest możliwe. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie nie jest możliwe, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń.</p> <p>Informuj. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.</p>
Typy plików	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> <p>Program Kaspersky Endpoint Security traktuje pliki bez rozszerzeń jak pliki wykonywalne. Kaspersky Endpoint Security zawsze skanuje pliki wykonywalne bez względu na typy plików wybrane do skanowania.</p> </div> <p>Wszystkie pliki. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia).</p> <p>Pliki skanowane według formatu. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował tylko infekowalne pliki . Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików.</p> <p>Pliki skanowane według rozszerzenia. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował tylko infekowalne pliki . Format pliku będzie określany w oparciu o jego rozszerzenie.</p> <p>Domyślnie program Kaspersky Endpoint Security skanuje pliki według ich formatu. Skanowanie plików według rozszerzenia jest mniej bezpieczne, ponieważ szkodliwy plik może mieć rozszerzenie, które nie znajduje się na liście potencjalnie infekowalnych (na przykład: .123).</p>
Skanuj tylko nowe i zmienione pliki	Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.
Pomiń pliki skanowane dłużej niż N s	Ogranicza czas skanowania pojedynczego obiektu. Po określonym czasie Kaspersky Endpoint Security przestanie skanować plik. To pomaga skrócić czas skanowania.
Skanuj archiwa	Skanuje archiwa w następujących formatach: RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
Skanuj pakiety	To pole włącza/wyłącza skanowanie pakietów dystrybucyjnych.

dystrybucyjne	
Skanuj pliki w formatach Microsoft Office	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty.
Skanuj formaty poczty elektronicznej	<p>Ta opcja włącza / wyłącza dla Kaspersky Endpoint Security opcję skanowania plików w formatach pocztowych i bazach danych poczty.</p> <p>Aplikacja całkowicie skanuje tylko formaty plików MS Outlook, Windows Mail/Outlook Express i EML i tylko wtedy, gdy na komputerze znajduje się klient poczty MS Outlook x86.</p> <p>Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security rozkłada pliki w formatach pocztowych na składniki (nagłówek, ciało, załączniki) i skanuje je w poszukiwaniu zagrożeń.</p> <p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki w formatach pocztowych jako pojedyncze pliki.</p>
Skanuj archiwa zabezpieczone hasłem	<p>Jeżeli pole jest zaznaczone, Kaspersky Endpoint Security skanuje archiwa zabezpieczone hasłem. Zanim pliki w archiwum zostaną przeskanowane, zostaniesz poproszony o wpisanie hasła.</p> <p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security pomija skanowanie archiwów chronionych hasłem.</p>
Nie rozpakowuj dużych plików złożonych	<p>Jeżeli to pole jest zaznaczone, Kaspersky Endpoint Security nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość.</p> <p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki złożone o wszystkich rozmiarach.</p> <p>Kaspersky Endpoint Security skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.</p>
Uczenie maszynowe i analiza sygnatur	<p>Metoda uczenia maszynowego i analiza sygnatur używa baz danych Kaspersky Endpoint Security, które zawierają opisy znanych zagrożeń oraz metody ich neutralizowania. Ochrona korzystająca z tej metody zapewnia minimalny dopuszczalny poziom ochrony.</p> <p>W oparciu o zalecenia ekspertów z Kaspersky, uczenie maszynowe i analiza sygnatur jest zawsze włączona.</p>
Analiza heurystyczna	<p>Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa.</p> <p>Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.</p>
Technologia iSwift	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczenie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.
Technologia iChecker	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczenie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest

rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).

Sprawdzanie integralności aplikacji

Kaspersky Endpoint Security sprawdza, czy moduły aplikacji nie są uszkodzone lub zmodyfikowane. Na przykład, jeśli biblioteka aplikacji posiada nieprawidłowy podpis cyfrowy, zostanie ona uznana za uszkodzoną. Zadanie *Sprawdzanie integralności* jest przeznaczone do skanowania plików. Uruchom zadanie *Sprawdzanie integralności*, jeśli program Kaspersky Endpoint Security wykrył szkodliwy obiekt, ale go nie zneutralizował.

Możesz utworzyć zadanie *Sprawdzanie integralności* tylko w konsoli Kaspersky Security Center Web Console i w Konsoli administracyjnej. Nie można utworzyć zadania w konsoli Kaspersky Security Center Cloud Console.

Naruszenia integralności aplikacji mogą pojawić się w następujących przypadkach:

- Szkodliwy obiekt zmodyfikował pliki Kaspersky Endpoint Security. W tym przypadku przeprowadź procedurę przywracania Kaspersky Endpoint Security przy pomocy narzędzi systemu operacyjnego. Po przywróceniu uruchom pełne skanowanie komputera i powtórz sprawdzanie integralności.
- Podpis cyfrowy utracił ważność. W tym przypadku zaktualizuj Kaspersky Endpoint Security.

[Jak uruchomić sprawdzanie integralności aplikacji za pomocą Konsoli administracyjnej \(MMC\)?](#) 

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zadania**.

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Nowe zadanie**.

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

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (11.7.0)** → **Sprawdzanie integralności**.

Krok 2. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

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

Krok 3. Konfigurowanie terminarza uruchamiania zadania

Skonfiguruj terminarz uruchamiania zadania, na przykład, ręcznie lub gdy wykrywana jest epidemia wirusów.

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład, `Sprawdzanie integralności po zainfekowaniu komputera`.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie Kreatora. W razie potrzeby zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania. W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał integralność aplikacji. Możesz także skonfigurować terminarz sprawdzania integralności aplikacji we właściwościach zadania (patrz tabela poniżej).

[Jak uruchomić sprawdzanie integralności aplikacji za pomocą konsoli Web Console? !\[\]\(41aea2746216b27a6939d696d8e035da_img.jpg\)](#)

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

b. Na liście rozwijanej **Typ zadania** wybierz **Sprawdzanie integralności**.

c. W polu **Nazwa zadania** wpisz krótki opis, na przykład: **Sprawdzanie integralności aplikacji po infekcji komputera**.

d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.

5. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

Nowe zadanie zostanie wyświetlone na liście zadań.

6. Zaznacz pole obok zadania.

W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał integralność aplikacji. Możesz także skonfigurować terminarz sprawdzania integralności aplikacji we właściwościach zadania (patrz tabela poniżej).

[Jak w interfejsie aplikacji uruchomić sprawdzanie integralności?](#)

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.

2. To spowoduje otwarcie listy zadań; wybierz zadanie *Sprawdzanie integralności* i kliknij **Uruchom skanowanie**.

W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał integralność aplikacji. Możesz także skonfigurować terminarz sprawdzania integralności aplikacji we właściwościach zadania (patrz tabela poniżej). Jeśli *Sprawdzanie integralności* nie jest wyświetlane, to oznacza, że administrator [zabronił używania zadań lokalnych w zasadzie](#).

Ustawienia zadania Sprawdzanie integralności

Parametr	Opis
Terminarz skanowania	Ręcznie. Tryb uruchamiania, w którym możesz ręcznie uruchomić skanowanie w wygodnym dla siebie momencie. Zgodnie z terminarzem. W tym trybie Kaspersky Endpoint Security uruchamia zadanie skanowania zgodnie z ustalonym terminarzem. Jeśli wybrano ten tryb uruchamiania, zadanie skanowania może również zostać uruchomione ręcznie.
Uruchom pominięte	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security uruchamia pominięte zadanie skanowania, kiedy tylko będzie to możliwe. Zadanie skanowania może zostać pominięte, na

zadania	przykład, jeśli komputer był wyłączony w zaplanowanym czasie uruchomienia zadania skanowania. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie uruchamia pominiętych zadań skanowania. Zamiast tego uruchomi następnne zadanie skanowania zgodnie z bieżącym terminarzem.
Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności	Odroczono uruchomienie zadania skanowania, gdy zasoby komputera są zajęte. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałes wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane.
Uruchom skanowanie jako <i>(dostępny tylko w Kaspersky Security Center Console)</i>	Domyślnie zadanie skanowania jest uruchamiane w imieniu użytkownika, z którego uprawnieniami jesteś zarejestrowany w systemie operacyjnym. W celu uzyskania dostępu do folderu instalacyjnego aplikacji wymagane mogą być odpowiednie uprawnienia. Możesz wskazać użytkownika, który posiada odpowiednie uprawnienia, w ustawieniach Kaspersky Endpoint Security i uruchomić skanowanie z poziomu konta tego użytkownika.

Modyfikowanie obszaru skanowania

Obszar skanowania to lista ścieżek do folderów oraz ścieżek, które Kaspersky Endpoint Security skanuje podczas wykonywania zadania. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki * i ?.

Aby edytować obszar skanowania, zalecane jest użycie zadania *Skanowanie obiektów*. Ekspert z Kaspersky zalecają, aby nie zmieniać obszaru skanowania zadania *Pełne skanowanie* i *Skanowanie obszarów krytycznych*.

Kaspersky Endpoint Security posiada następujące predefiniowane obiekty jako część obszaru skanowania:

- **Moja poczta.**
Pliki odpowiednie dla klienta pocztowego Outlook: pliki danych (PST), pliki danych offline (OST).
- **Pamięć jądra.**
- **Uruchomione procesy i obiekty startowe.**
Pamięć zajęta przez procesy i pliki wykonywalne aplikacji, które są uruchamiane przy starcie systemu.
- **Sektory startowe dysków.**
Sektory startowe dysków wymiennych i dysku twardego.
- **Kopia zapasowa systemu.**
Zawartość folderu informacji o woluminie systemowym.
- **Wszystkie dyski wymienne.**
- **Wszystkie dyski twarde.**
- **Wszystkie dyski sieciowe.**

Aby wykluczyć foldery lub pliki z obszaru skanowania, [dodaj folder lub plik do strefy zaufanej](#).

[Jak w Konsoli administracyjnej \(MMC\) edytować obszar skanowania?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zadania**.
4. Wybierz zadanie skanowania i kliknij je dwukrotnie, aby otworzyć właściwości zadania.
Jeśli to konieczne, [utwórz zadanie Skanowanie antywirusowe](#).
5. W oknie właściwości zadania wybierz sekcję **Ustawienia**.
6. W sekcji **Obszar skanowania** kliknij **Ustawienia**.
7. W otwartym oknie wybierz obiekty, które chcesz dodać do obszaru skanowania lub wykluczyć z niego.
8. Jeśli chcesz dodać nowy obiekt do obszaru skanowania:
 - a. Kliknij przycisk **Dodaj**.
 - b. W polu **Obiekt** wprowadź ścieżkę do folderu lub pliku i kliknij **Dodaj**.

Użyj masek:

- Znak ***** (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:**.txt** będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
- Dwa występujące po sobie znaki ****** zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:\Folder***.txt** będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie **Folder** i w jego podfolderach. Maskę musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maskę **C:***.txt** nie jest ważną maską.
- Znak **?** (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:\Folder\???.txt** będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie **Folder**, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

Możesz wykluczyć obiekt ze skanowań bez usuwania go z listy obiektów w obszarze skanowania. W tym celu odznacz pole obok obiektu.

9. Zapisz swoje zmiany.

[Jak w konsoli Web Console i Cloud Console edytować obszar skanowania?](#)

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

Zostanie otwarta lista zadań.

2. Kliknij zadanie skanowania.

Zostanie otwarte okno właściwości zadania. Jeśli to konieczne, [utwórz zadanie Skanowanie antywirusowe](#).

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. W sekcji **Obszar skanowania** wybierz obiekty, które chcesz dodać do obszaru skanowania lub wykluczyć z niego.

5. Jeśli chcesz dodać nowy obiekt do obszaru skanowania:

a. Kliknij przycisk **Dodaj**.

b. W polu **Ścieżka dostępu** wprowadź ścieżkę do folderu lub pliku i kliknij **OK**.

Użyj masek:

- Znak ***** (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:**.txt** będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
- Dwa występujące po sobie znaki ****** zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:\Folder***.txt** będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie **Folder** i w jego podfolderach. Maskę musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maskę **C:***.txt** nie jest ważną maską.
- Znak **?** (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:\Folder\???.txt** będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie **Folder**, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

Możesz wykluczyć obiekt ze skanowań bez usuwania go z listy obiektów w obszarze skanowania. W tym celu ustaw przycisk przełącznika obok obiektu na pozycję wyłączenia.

6. Zapisz swoje zmiany.

[Jak w interfejsie aplikacji edytować obszar skanowania?](#)

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.

2. Na liście zadań wybierz zadanie *Skanowanie obiektów* i kliknij **Wybierz**.

Możesz także edytować obszar skanowania dla innych zadań. Ekspersi z Kaspersky zalecają, aby nie zmieniać obszaru skanowania zadania *Pełne skanowanie* i *Skanowanie obszarów krytycznych*.

3. W otwartym oknie wybierz obiekty, które chcesz dodać do obszaru skanowania.

4. Zapisz swoje zmiany.

Jeśli zadanie skanowania nie jest wyświetlane, oznacza to, że administrator [zabronił użycia zadań lokalnych w zasadzie](#).

Uruchamianie zaplanowanego skanowania

Pełne skanowanie komputera zajmuje sporo czasu i wymaga dużej ilości zasobów komputera. Powinieneś wybrać optymalny czas uruchomienia skanowania komputera, aby uniknąć szkodliwego wpływu na działanie innego oprogramowania. Kaspersky Endpoint Security umożliwia skonfigurowanie normalnego terminarza skanowania komputera. To jest odpowiednie, jeśli Twoja organizacja posiada plan pracy. Możesz skonfigurować uruchamianie skanowania komputera w nocy lub w weekendy. Jeżeli z jakiegoś powodu uruchomienie zadania nie będzie możliwe (na przykład komputer nie będzie włączony o określonym czasie), można skonfigurować automatyczne uruchamianie pominiętego zadania przy najbliższej możliwej okazji.

Jeśli skonfigurowanie optymalnego terminarza skanowania okazuje się niemożliwe, Kaspersky Endpoint Security umożliwia uruchomienie skanowania komputera, gdy spełnione są następujące specjalne warunki:

- Po aktualizacji baz danych.

Kaspersky Endpoint Security uruchamia skanowanie komputera wraz z zaktualizowanymi bazami danych.

- Po uruchomieniu aplikacji.

Kaspersky Endpoint Security uruchamia skanowanie komputera, gdy od uruchomienia aplikacji minie określony czas. Przy uruchamianiu systemu operacyjnego wiele procesów jest uruchomionych, dlatego korzystne jest odroczenie uruchomienia zadania skanowania zamiast uruchomienie do od razu po uruchomieniu Kaspersky Endpoint Security.

- Wake-on-LAN.

Kaspersky Endpoint Security uruchamia skanowanie komputera zgodnie z terminarzem nawet wtedy, gdy komputer jest wyłączony. Aby to zrobić, aplikacja używa funkcji Wake-on-LAN systemu operacyjnego. Funkcja Wake-on-LAN umożliwia zdalne włączenie komputera poprzez wysłanie specjalnego sygnału przez sieć lokalną. Aby użyć tej funkcji, musisz włączyć Wake-on-LAN w ustawieniach BIOS-u.

Możesz skonfigurować uruchamianie skanowania przy użyciu Wake-on-LAN tylko dla zadania *Skanowanie antywirusowe* w Kaspersky Security Center. Nie możesz włączyć Wake-on-LAN dla skanowania komputera w interfejsie aplikacji.

- Kiedy komputer jest w stanie bezczynności.

Kaspersky Endpoint Security uruchamia skanowanie komputera zgodnie z terminarzem, gdy wygaszacz ekranu jest aktywny lub ekran jest zablokowany. Jeśli użytkownik odblokuje komputer, Kaspersky Endpoint Security wstrzyma skanowanie. To oznacza, że pełne skanowanie komputera może potrwać kilka dni.

[Jak w Konsoli administracyjnej \(MMC\) skonfigurować terminarz skanowania?](#) 


1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zadania**.
4. Wybierz zadanie skanowania i kliknij je dwukrotnie, aby otworzyć właściwości zadania.
Jeśli to konieczne, [utwórz zadanie Skanowanie antywirusowe](#).
5. W oknie właściwości zadania wybierz sekcję **Terminarz**.
6. Skonfiguruj terminarz zadania skanowania.
7. W zależności od wybranej częstotliwości, skonfiguruj ustawienia zaawansowane, które określają terminarz uruchamiania zadania (patrz tabela poniżej).
8. Zapisz swoje zmiany.

[Jak w konsoli Web Console i Cloud Console skonfigurować terminarz skanowania?](#) ⓘ

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Kliknij zadanie skanowania.
Zostanie otwarte okno właściwości zadania.
3. Wybierz zakładkę **Terminarz**.
4. Skonfiguruj terminarz zadania skanowania.
5. W zależności od wybranej częstotliwości, skonfiguruj ustawienia zaawansowane, które określają terminarz uruchamiania zadania (patrz tabela poniżej).
6. Zapisz swoje zmiany.

[Jak w interfejsie aplikacji skonfigurować terminarz skanowania?](#) ⓘ

Możesz skonfigurować terminarz skanowania tylko wtedy, gdy zasada nie jest stosowana do komputera. Dla komputerów pracujących pod kontrolą zasady możesz skonfigurować terminarz zadania *Skanowanie antywirusowe* w Kaspersky Security Center.

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij .
Możesz skonfigurować terminarz uruchamiania Pełnego skanowania, Skanowania obszarów krytycznych lub Sprawdzania integralności. Możesz tylko ręcznie uruchomić Skanowanie obiektów.
3. Kliknij przycisk **Terminarz skanowania**.
4. W otwartym oknie skonfiguruj terminarz uruchamiania zadania skanowania.
5. W zależności od wybranej częstotliwości, skonfiguruj ustawienia zaawansowane, które określają terminarz uruchamiania zadania (patrz tabela poniżej).
6. Zapisz swoje zmiany.

Ustawienia terminarza skanowania

Parametr	Opis
Terminarz skanowania	Ręcznie. Tryb uruchamiania, w którym możesz ręcznie uruchomić skanowanie w wygodnym dla siebie momencie. Zgodnie z terminarzem. W tym trybie Kaspersky Endpoint Security uruchamia zadanie skanowania zgodnie z ustalonym terminarzem. Jeśli wybrano ten tryb uruchamiania, zadanie skanowania może również zostać uruchomione ręcznie.
Uruchom po N minutach od uruchomienia aplikacji	Odroczone uruchomienie zadania skanowania po uruchomieniu aplikacji. Przy uruchamianiu systemu operacyjnego wiele procesów jest uruchomionych, dlatego korzystne jest odroczenie uruchomienia zadania skanowania zamiast uruchomienie do od razu po uruchomieniu Kaspersky Endpoint Security.
Uruchom pominięte zadania	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security uruchamia pominięte zadanie skanowania, kiedy tylko będzie to możliwe. Zadanie skanowania może zostać pominięte, na przykład, jeśli komputer był wyłączony w zaplanowanym czasie uruchomienia zadania skanowania. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie uruchamia pominiętych zadań skanowania. Zamiast tego uruchomi następane zadanie skanowania zgodnie z bieżącym terminarzem.
Uruchamiaj tylko, jeśli komputer jest w stanie bezczynności	Odroczono uruchomienie zadania skanowania, gdy zasoby komputera są zajęte. Kaspersky Endpoint Security uruchamia zadanie skanowania, jeśli komputer jest zablokowany lub wygaszacz ekranu jest włączony. Jeśli przerwałeś wykonywanie zadania, na przykład, poprzez odblokowanie komputera, Kaspersky Endpoint Security automatycznie uruchamia zadanie, kontynuując od momentu, w którym zostało przerwane.
Używaj automatycznie losowego opóźnienia dla uruchamiania zadań	Jeśli pole jest zaznaczone, zadanie nie jest uruchamiane ściśle zgodnie z terminarzem, ale losowo w obrębie pewnego przedziału czasu, czyli czasy uruchomień zadania są rozłożone w czasie. Losowe czasy uruchomień pomagają w uniknięciu dostępu do Serwera administracyjnego przez znaczną liczbę komputerów jednocześnie, gdy zadanie jest uruchomione zgodnie z terminarzem.

<p><i>(dostępny tylko w Kaspersky Security Center Console)</i></p>	<p>Zakres losowych czasów uruchomień jest automatycznie wyliczany po utworzeniu zadania, w zależności od liczby komputerów, do których przypisano zadanie. Następnie zadanie jest zawsze uruchamiane w wyliczonym czasie uruchomienia. Jednakże za każdym razem, gdy ustawienia zadania są modyfikowane lub zadanie jest uruchamiane ręcznie, obliczony czas uruchomienia zmienia się.</p> <p>Jeśli pole jest odznaczone, zadanie jest uruchamiane dokładnie o zaplanowanym czasie.</p>
<p>Włącz urządzenie przed uruchomieniem zadania przy użyciu funkcji Wake-on-LAN (min)</p> <p><i>(dostępny tylko w Kaspersky Security Center Console)</i></p>	<p>Jeśli pole jest zaznaczone, system operacyjny komputera ma określony czas realizacji na zakończenie uruchamiania przed uruchomieniem zadania. Domyślny czas realizacji wynosi 5 minut.</p> <p>Zaznacz pole, jeśli chcesz uruchomić zadanie na wszystkich komputerach, w tym wyłączonych komputerach.</p>

Uruchamianie skanowania jako inny użytkownik

Domyślnie zadanie skanowania jest uruchamiane w imieniu użytkownika, z którego uprawnieniami jesteś zarejestrowany w systemie operacyjnym. Obszar ochrony może zawierać dyski sieciowe lub inne obiekty, które wymagają specjalnych uprawnień dostępu. Możesz wskazać użytkownika, który posiada odpowiednie uprawnienia, w ustawieniach Kaspersky Endpoint Security i uruchomić skanowanie z poziomu konta tego użytkownika.

Jako inny użytkownik możesz uruchomić następujące skanowania:

- Skanowanie obszarów krytycznych.
- Pełne skanowanie.
- Skanowanie obiektów.
- [Skanowanie z menu kontekstowego](#).

Nie możesz skonfigurować uprawnień użytkownika do uruchomienia [Skanowania dysków wymiennych](#), [Skanowania w tle](#) lub [Sprawdzania integralności](#).


[Jak w Konsoli administracyjnej \(MMC\) uruchomić skanowanie jako inny użytkownik?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zadania**.
4. Wybierz zadanie skanowania i kliknij je dwukrotnie, aby otworzyć właściwości zadania.
5. W oknie właściwości zadania wybierz sekcję **Konto**.
6. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania skanowania.
7. Zapisz swoje zmiany.

Jak w konsoli Web Console lub Cloud Console uruchomić skanowanie jako inny użytkownik?

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Kliknij zadanie skanowania.
Zostanie otwarte okno właściwości zadania.
3. Wybierz zakładkę **Ustawienia**.
4. W sekcji **Konto** kliknij **Ustawienia**.
5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania skanowania.
6. Zapisz swoje zmiany.

Jak w interfejsie aplikacji uruchomić skanowanie jako inny użytkownik?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij .
3. Kliknij **Ustawienia zaawansowane** → **Uruchom skanowanie jako**.
4. W otwartym oknie wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania skanowania.
5. Zapisz swoje zmiany.

Jeśli zadanie skanowania nie jest wyświetlane, oznacza to, że administrator [zabronił użycia zadań lokalnych w zasadzie](#).

Optymalizacja skanowania

Możesz zoptymalizować skanowanie plików, zmniejszając czas skanowania i zwiększając szybkość działania programu Kaspersky Endpoint Security. Można to uzyskać poprzez skanowanie tylko nowych plików i tych plików, które zostały zmodyfikowane od ostatniego skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych. Możesz również ustawić ograniczenie skanowania pojedynczego pliku. Po upływie określonego czasu, obiekt zostanie wykluczony z bieżącego skanowania (poza archiwami i plikami zawierającymi wiele obiektów).

Popularną techniką ukrywania wirusów i innego szkodliwego oprogramowania jest osadzanie ich w plikach złożonych, takich jak archiwa czy bazy danych. W celu wykrycia ukrytych w ten sposób wirusów i innego szkodliwego oprogramowania, plik złożony musi zostać rozpakowany, co może spowolnić skanowanie. Możesz ograniczyć typy skanowanych plików złożonych, dzięki czemu skanowanie będzie szybsze.

Możesz także włączyć technologie: iChecker i iSwift. Technologie iChecker i iSwift optymalizują prędkość skanowania plików poprzez wykluczenie plików, które nie zostały zmodyfikowane od ostatniego skanowania.

[Jak w Konsoli administracyjnej \(MMC\) zoptymalizować skanowanie?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zadania**.
4. Wybierz zadanie skanowania i kliknij je dwukrotnie, aby otworzyć właściwości zadania.
Jeśli to konieczne, [utwórz zadanie Skanowanie antywirusowe](#).
5. W oknie właściwości zadania wybierz sekcję **Ustawienia**.
6. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
To spowoduje otwarcie okna ustawień zadania skanowania.
7. W sekcji **Optimalizacja skanowania** skonfiguruj ustawienia skanowania:
 - **Skanuj tylko nowe i zmienione pliki**. Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.
Możesz także skonfigurować skanowanie nowych plików według typu. Na przykład, możesz przeskanować wszystkie pakiety dystrybucyjne i przeskanować tylko nowe archiwa i pliki formatów office.
 - **Pomiń pliki skanowane dłużej niż N s**. Ta opcja ustawia limit czasu skanowania pojedynczego obiektu. Po określonym czasie Kaspersky Endpoint Security przestanie skanować plik. To pomaga skrócić czas skanowania.
8. Kliknij przycisk **Dodatkowe**.
To spowoduje otwarcie okna ustawień skanowania plików złożonych.
9. W sekcji **Ograniczenie rozmiaru** zaznacz pole **Nie rozpakowuj dużych plików złożonych**. Ogranicza czas skanowania pojedynczego obiektu. Po określonym czasie Kaspersky Endpoint Security przestanie skanować plik. To pomaga skrócić czas skanowania.

Kaspersky Endpoint Security skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

10. Kliknij **OK**.
11. Wybierz zakładkę **Dodatkowe**.
12. W sekcji **Technologie skanowania** zaznacz pola obok nazw technologii, których chcesz użyć podczas skanowania:
 - **Technologia iSwift**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczenie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.

- **Technologia iChecker.** Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczenie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).

13. Zapisz swoje zmiany.

Jak w konsoli Web Console i Cloud Console zoptymalizować skanowanie?

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

Zostanie otwarta lista zadań.

2. Kliknij zadanie skanowania.

Zostanie otwarte okno właściwości zadania. Jeśli to konieczne, [utwórz zadanie *Skanowanie antywirusowe*](#).

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. W sekcji **Działanie podejmowane w przypadku wykrycia zagrożenia** zaznacz pole **Skanuj tylko nowe i zmienione pliki**. Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.

Możesz także skonfigurować skanowanie nowych plików według typu. Na przykład, możesz przeskanować wszystkie pakiety dystrybucyjne i przeskanować tylko nowe archiwa i pliki formatów office.


5. Zaznacz pole **Nie rozpakowuj dużych plików złożonych**. Ogranicza czas skanowania pojedynczego obiektu. Po określonym czasie Kaspersky Endpoint Security przestanie skanować plik. To pomaga skrócić czas skanowania.

Kaspersky Endpoint Security skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

6. W sekcji **Ustawienia zaawansowane** zaznacz pole **Pomiń pliki skanowane dłużej niż N s**. To powoduje ustawienie ograniczenia czasu skanowania pojedynczego obiektu. Po określonym czasie Kaspersky Endpoint Security przestanie skanować plik. To pomaga skrócić czas skanowania.

7. Zapisz swoje zmiany.

Jak w interfejsie aplikacji zoptymalizować skanowanie?

1. W oknie głównym aplikacji przejdź do sekcji **Zadania**.
2. Na liście zadań wybierz zadanie skanowania i kliknij .
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. W sekcji **Optymalizacja skanowania** skonfiguruj ustawienia skanowania:
 - **Skanuj tylko nowe i zmienione pliki**. Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.
Możesz także skonfigurować skanowanie nowych plików według typu. Na przykład, możesz przeskanować wszystkie pakiety dystrybucyjne i przeskanować tylko nowe archiwa i pliki formatów office.
 - **Pomiń pliki skanowane dłużej niż N s**. Ta opcja ustawia limit czasu skanowania pojedynczego obiektu. Po określonym czasie Kaspersky Endpoint Security przestanie skanować plik. To pomaga skrócić czas skanowania.
5. W sekcji **Ograniczenie rozmiaru** zaznacz pole **Nie rozpakowuj dużych plików złożonych**. Ogranicza czas skanowania pojedynczego obiektu. Po określonym czasie Kaspersky Endpoint Security przestanie skanować plik. To pomaga skrócić czas skanowania.

Kaspersky Endpoint Security skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

6. W sekcji **Technologie skanowania** zaznacz pola obok nazw technologii, których chcesz użyć podczas skanowania:
 - **Technologia iSwift**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczenie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.
 - **Technologia iChecker**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczenie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).
7. Zapisz swoje zmiany.

Jeśli zadanie skanowania nie jest wyświetlane, oznacza to, że administrator [zabronił użycia zadań lokalnych w zasadzie](#).

Aktualizowanie baz danych i modułów aplikacji

Aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security zapewnia aktualną ochronę Twojego komputera. Codziennie na całym świecie pojawia się duża ilość nowych wirusów i innego typu szkodliwego oprogramowania. Bazy danych Kaspersky Endpoint Security zawierają informacje o zagrożeniach i sposoby ich neutralizowania. Aby szybko wykrywać zagrożenia, zalecamy regularnie aktualizować bazy danych i moduły aplikacji.

Regularne aktualizacje wymagają ważnej licencji na aplikację. Jeżeli nie ma bieżącej licencji, wówczas możliwe będzie wykonanie tylko jednej aktualizacji.

Głównym źródłem uaktualnień dla Kaspersky Endpoint Security są serwery aktualizacji firmy Kaspersky.

Aby możliwe było pobieranie pakietów aktualizacji z serwerów aktualizacji Kaspersky, komputer musi być podłączony do internetu. Domyślnie ustawienia połączenia internetowego są określone automatycznie. Jeśli korzystasz z serwera proxy, konieczne może być dostosowanie ustawień serwera proxy.

Uaktualnienia są pobierane po protokole HTTPS. Mogą także zostać pobrane po protokole HTTP, jeśli niemożliwe jest pobranie uaktualnień po protokole HTTPS.

Podczas procesu aktualizacji, na komputer są pobierane i instalowane następujące obiekty:

- Bazy danych programu Kaspersky Endpoint Security. Ochrona komputera jest zapewniana przy pomocy baz danych zawierających sygnatury wirusów i innych zagrożeń oraz informacje o sposobach ich neutralizacji. Moduły ochrony korzystają z tych informacji przy wyszukiwaniu i neutralizowaniu zainfekowanych plików na Twoim komputerze. Bazy danych są ciągle aktualizowane o wpisy nowych zagrożeń i metody ich zwalczania. Dlatego zalecamy regularne aktualizowanie baz danych.
Oprócz baz danych Kaspersky Endpoint Security aktualizowane są również sterowniki sieciowe, które umożliwiają modułom aplikacji przechwytywanie ruchu sieciowego.
- Moduły aplikacji. Oprócz baz danych aplikacji można także aktualizować jej moduły. Aktualizowanie modułów aplikacji likwiduje luki w Kaspersky Endpoint Security, dodaje nowe funkcje lub poprawia te istniejące.

Podczas aktualizacji moduły i bazy danych aplikacji znajdujące się na komputerze porównywane są z tymi aktualnymi, znajdującymi się w źródle uaktualnień. Jeśli Twoje bieżące bazy danych i moduły różnią się od najnowszych wersji, na Twoim komputerze zainstalowana zostanie brakująca część uaktualnień.

Pliki pomocy kontekstowej mogą być aktualizowane wraz z modułami aplikacji.

Jeśli bazy danych są bardzo stare, pakiet uaktualnień może być duży, co spowoduje zwiększony ruch internetowy (kilkadziesiąt MB).

Informacje o bieżącym stanie baz danych Kaspersky Endpoint Security jest wyświetlany w oknie głównym aplikacji lub w dymku, który jest wyświetlany po najechaniu kursorem na ikonę aplikacji w obszarze powiadomień.

Informacje o wynikach aktualizacji i wszystkich zdarzeniach zaistniałych podczas wykonywania zadania aktualizacji zapisywane są w [raporcie Kaspersky Endpoint Security](#).

Scenariusze aktualizacji baz danych i modułów aplikacji

Aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security zapewnia aktualną ochronę Twojego komputera. Codziennie na całym świecie pojawia się duża ilość nowych wirusów i innego typu szkodliwego oprogramowania. Bazy danych Kaspersky Endpoint Security zawierają informacje o zagrożeniach i sposoby ich neutralizowania. Aby szybko wykrywać zagrożenia, zalecamy regularnie aktualizować bazy danych i moduły aplikacji.

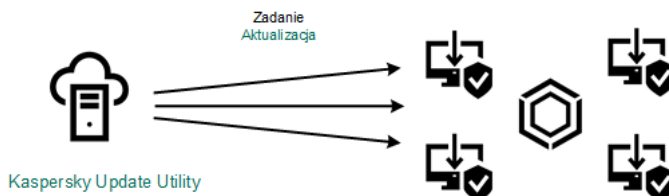
Na komputerach użytkowników aktualizowane są następujące obiekty:

- Antywirusowe bazy danych. Antywirusowe bazy danych zawierają bazy danych sygnatur szkodliwych programów, opisy ataków sieciowych, bazy danych szkodliwych i phishingowych adresów internetowych, bazy danych banerów, bazy danych spamu oraz inne dane.
- Moduły aplikacji. Aktualizacje modułów są przeznaczone do eliminowania luk w aplikacji i do udoskonalania metod ochrony komputera. Aktualizacje modułów mogą zmieniać zachowanie komponentów aplikacji i dodawać nowe możliwości.

Kaspersky Endpoint Security obsługuje następujące scenariusze aktualizowania baz danych i modułów:

- Aktualizacja z serwerów Kaspersky.

Serwery aktualizacji Kaspersky znajdują się w różnych krajach na całym świecie. To zapewnia wysoką niezawodność aktualizacji. Jeśli aktualizacja nie może zostać wykonana z jednego serwera, Kaspersky Endpoint Security przełączy się do kolejnego serwera.



Aktualizacja z serwerów Kaspersky

- Scentralizowana aktualizacja.

Scentralizowana aktualizacja zmniejsza zewnętrzny ruch internetowy i zapewnia wygodne monitorowanie aktualizacji.

Scentralizowana aktualizacja składa się na następujące kroki:

1. Pobierz pakiet aktualizacji do repozytorium w obrębie sieci organizacji.

Pakiet aktualizacji jest pobierany do repozytorium przez zadanie Serwera administracyjnego o nazwie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*.

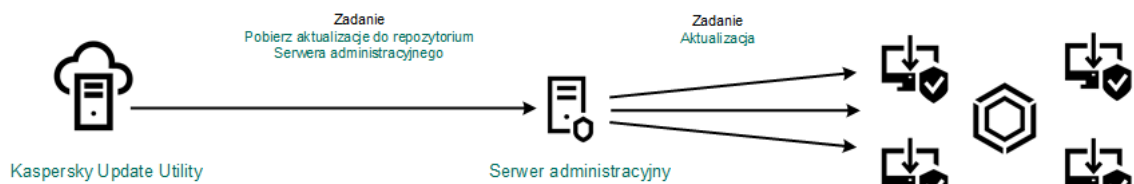
2. Pobierz pakiet aktualizacji do folderu współdzielonego (opcjonalnie).

Pakiet aktualizacji można pobrać do folderu współdzielonego, korzystając z następujących metod:

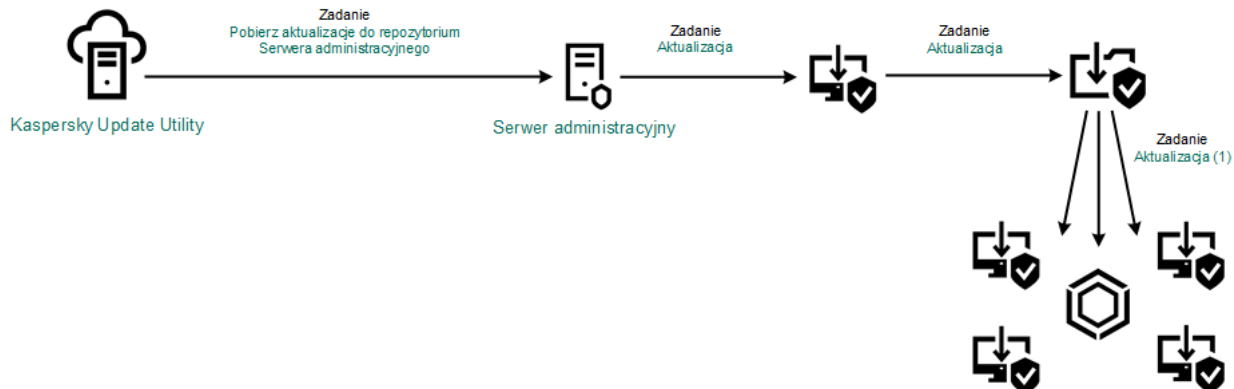
- Korzystając z zadania *Aktualizacja* programu Kaspersky Endpoint Security. Zadanie jest przeznaczone dla jednego z komputerów w lokalnej sieci komputerowej.
- Przy użyciu narzędzia Kaspersky Update Utility. Szczegółowe informacje na temat korzystania z narzędzia Kaspersky Update Utility znajdziesz w [Bazie wiedzy Kaspersky](#).

3. Roześlij pakiet aktualizacji na komputery klienckie.

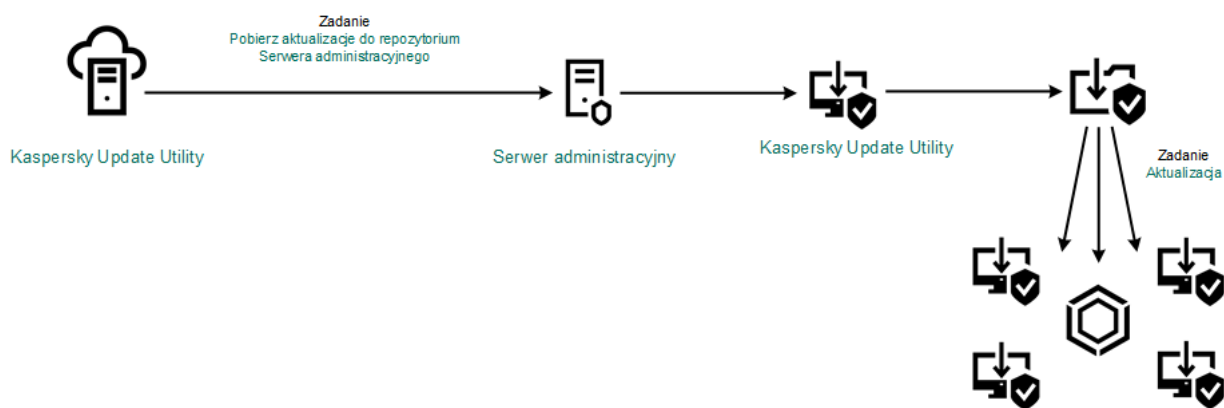
Pakiet aktualizacji jest rozesyłany na komputery klienckie przez zadanie *Aktualizacja* programu Kaspersky Endpoint Security. Dla każdej grupy administracyjnej możesz utworzyć nieograniczoną liczbę zadań aktualizacji.



Aktualizowanie z repozytorium serwera



Aktualizowanie z folderu współdzielonego



Aktualizowanie przy użyciu narzędzia Kaspersky Update Utility

Dla konsoli Web Console domyślna lista źródeł uaktualnień zawiera Serwer administracyjny Kaspersky Security Center i serwery aktualizacji Kaspersky. W przypadku konsoli Kaspersky Security Center Cloud Console domyślna lista źródeł uaktualnień zawiera punkty dystrybucji i serwery aktualizacji Kaspersky. Więcej informacji o punktach dystrybucji znajdziesz w *pomocy do Kaspersky Security Center Cloud Console*. Do listy można dodać inne źródło uaktualnień. Źródłem uaktualnień mogą być serwery HTTP/FTP oraz foldery współdzielone. Jeśli aktualizacja nie może zostać wykonana z jednego źródła uaktualnień, Kaspersky Endpoint Security przełączy się do kolejnego serwera.

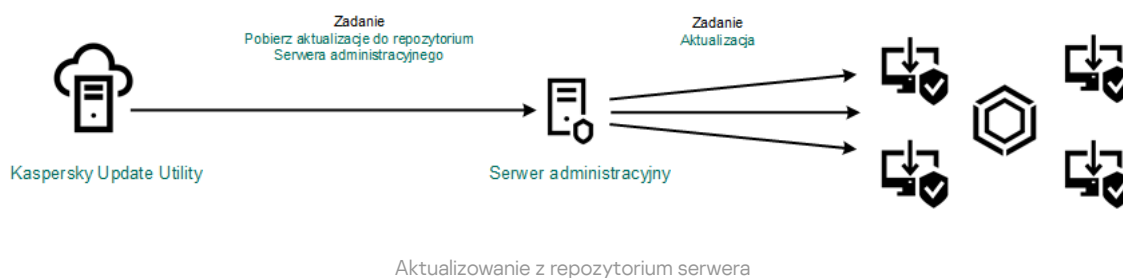
Uaktualnienia są pobierane z serwerów aktualizacji Kaspersky lub z innych serwerów FTP lub HTTP za pośrednictwem standardowych protokołów sieciowych. Jeśli do uzyskania dostępu do serwerów aktualizacji wymagane jest połączenie z serwerem proxy, [w ustawieniach profilu Kaspersky Endpoint Security określ ustawienia serwera proxy](#).

Aktualizowanie z repozytorium serwera

Aby oszczędzić ruch sieciowy, możesz skonfigurować aktualizacje baz danych i modułów aplikacji na komputerach sieci LAN organizacji z repozytorium serwera. W tym celu Kaspersky Security Center musi pobrać pakiet aktualizacyjny do repozytorium (serwer FTP lub HTTP, folder sieciowy lub lokalny) z serwerów aktualizacji Kaspersky. Pozostałe komputery w sieci LAN organizacji będą mogły pobierać pakiety aktualizacyjne z repozytorium serwera.

Konfigurowanie aktualizacji baz danych i modułów aplikacji z repozytorium serwera obejmuje następujące kroki:

1. Konfigurację pobrania pakietu aktualizacji do repozytorium Serwera administracyjnego (zadanie *Pobierz uaktualnienia do repozytorium Serwera administracyjnego*).
2. Konfigurację aktualizacji baz danych i modułów aplikacji z określonego repozytorium serwera do pozostałych komputerów w sieci LAN organizacji (zadanie *Aktualizacja*).



W celu skonfigurowania pobrania pakietu aktualizacji do repozytorium serwera:

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Wybierz zadanie **Pobierz aktualizacje do repozytorium Serwera administracyjnego**.
Zostanie otwarte okno właściwości zadania.
Zadanie *Pobierz aktualizacje do repozytorium Serwera administracyjnego* jest tworzone automatycznie przez Kreator wstępnej konfiguracji Kaspersky Security Center Web Console, a to zadanie może mieć tylko jedną instancję.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. W sekcji **Inne ustawienia** kliknij **Konfiguruj**.
5. W polu **Folder do przechowywania aktualizacji** określ adres serwera FTP lub HTTP, folderu sieciowego lub lokalnego, do którego Kaspersky Security Center skopiuje pakiet aktualizacji, pobrany z serwerów aktualizacji Kaspersky.

Dla źródła uaktualnień używany jest następujący format ścieżki dostępu:

- Dla serwera FTP lub HTTP wprowadź jego adres internetowy lub adres IP.
Na przykład: `http://dn1-01.geo.kaspersky.com/` lub `93.191.13.103`.
Dla serwera FTP możesz określić ustawienia autoryzacji w adresie internetowym, w następującym formacie:
`ftp://<nazwa_użytkownika>:<hasło>@<węzeł>:<port>`.
- Dla folderu sieciowego wprowadź ścieżkę UNC.
Na przykład: `\\ Server\Share\Update distribution`.
- Dla folderu lokalnego wprowadź pełną ścieżkę do tego folderu.
Na przykład: `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Zapisz swoje zmiany.

W celu skonfigurowania aktualizacji Kaspersky Endpoint Security z określonego repozytorium serwera:

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

Zostanie otwarta lista zadań.

2. Kliknij zadanie **Aktualizacja** dla Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości zadania.

Zadanie *Aktualizacja* jest tworzone automatycznie przez Kreator wstępnej konfiguracji programu Kaspersky Security Center. Aby utworzyć zadanie *Aktualizacja*, zainstaluj wtyczkę webową Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb lokalny**.

4. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.

5. W polu **Źródło** określ adres serwera FTP lub HTTP, folderu sieciowego lub lokalnego, do którego Kaspersky Security Center skopiuje pakiet aktualizacji, pobrany z serwerów Kaspersky.

Adres źródła uaktualnień musi odpowiadać adresowi określonymu w polu **Folder do przechowywania aktualizacji**, gdy skonfigurowałeś pobieranie uaktualnień do repozytorium serwera (patrz *powyższa instrukcja*).

6. W sekcji **Stan** wybierz **Włączono**.

7. Kliknij **OK**.

8. Skonfiguruj priorytety źródeł uaktualnień, korzystając z przycisków **W górę** i **W dół**.

9. Zapisz swoje zmiany.

Jeśli aktualizacja nie może zostać wykonana z pierwszego źródła uaktualnień, Kaspersky Endpoint Security automatycznie przełączy się do kolejnego źródła.

Aktualizowanie z folderu współdzielonego

Aby oszczędzić ruch sieciowy, możesz skonfigurować aktualizacje baz danych i modułów aplikacji na komputerach sieci LAN organizacji z folderu współdzielonego. W tym celu jeden z komputerów w sieci LAN organizacji musi odbierać pakiety aktualizacji z Serwera administracyjnego Kaspersky Security Center lub z serwerów aktualizacji Kaspersky i kopiować je do folderu współdzielonego. Pozostałe komputery w sieci LAN organizacji będą mogły pobrać pakiety aktualizacji z tego folderu współdzielonego.

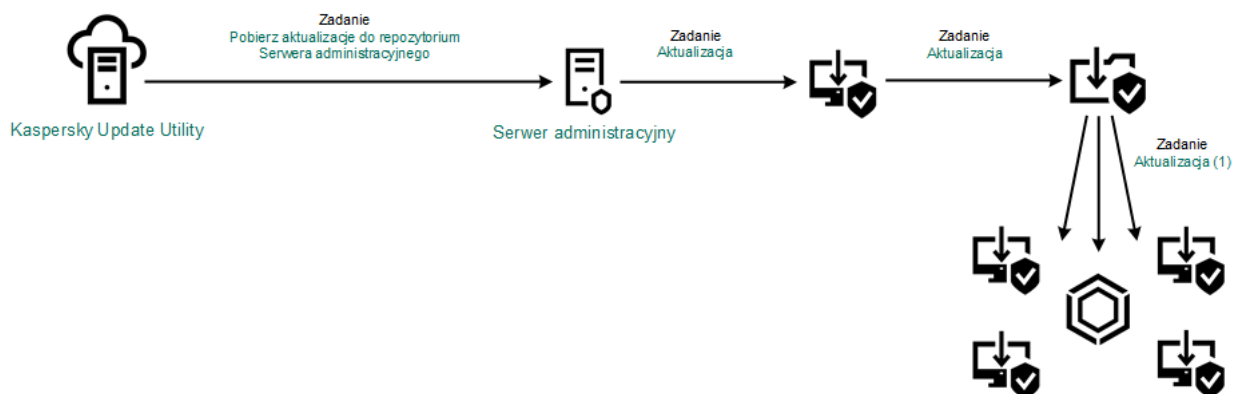
Konfigurowanie aktualizacji baz danych i modułów aplikacji z folderu współdzielonego obejmuje następujące kroki:

1. [Konfigurowanie aktualizacji baz danych i modułów aplikacji z repozytorium serwera](#).

2. Włącz kopiowanie pakietu uaktualnień do folderu współdzielonego na jednym z komputerów w firmowej sieci LAN (patrz poniższe instrukcje).

3. Konfiguruj aktualizację baz danych i modułów aplikacji z określonego folderu współdzielonego do pozostałych komputerów w firmowej sieci LAN (patrz poniższe instrukcje).

Wersja i lokalizacja aplikacji Kaspersky Endpoint Security, która kopiuje pakiet aktualizacyjny do folderu współdzielonego, musi odpowiadać wersji i lokalizacji aplikacji, która aktualizuje bazy danych z folderu współdzielonego. Jeśli wersje lub lokalizacje aplikacji nie odpowiadają, aktualizacja baz danych może zakończyć się błędem.



Aktualizowanie z folderu współdzielonego

W celu włączenia kopiowanie pakietu uaktualnień do foldera współdzielonego:

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

Zostanie otwarta lista zadań.

2. Kliknij zadanie **Aktualizacja** dla Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości zadania.

Zadanie *Aktualizacja* jest tworzone automatycznie przez Kreator wstępnej konfiguracji programu Kaspersky Security Center. Aby utworzyć zadanie *Aktualizacja*, zainstaluj wtyczkę webową Kaspersky Endpoint Security for Windows podczas działania kreatora.

3. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb lokalny**.

4. Skonfiguruj źródła uaktualnień.

Źródłami uaktualnień mogą być serwery aktualizacji Kaspersky, Serwer administracyjny Kaspersky Security Center, inne serwery FTP lub HTTP, foldery lokalne lub foldery sieciowe.

5. Zaznacz pole **Kopiuj aktualizacje do folderu**.

6. W polu **Ścieżka** wprowadź ścieżkę UNC do folderu współdzielonego (na przykład: \\Server\Share\Update distribution).

Jeśli pole pozostanie puste, Kaspersky Endpoint Security skopiuje pakiet aktualizacji do folderu C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\.

7. Zapisz swoje zmiany.

Zadanie *Aktualizacja* musi zostać przypisane do jednego komputera, który będzie pełnił rolę źródła uaktualnień.

W celu skonfigurowania aktualizacji z folderu współdzielonego:

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

b. Na liście rozwijalnej **Typ zadania** wybierz **Aktualizuj**.

c. W polu **Nazwa zadania** wpisz krótki opis, na przykład, **Aktualizowanie z folderu współdzielonego**.

d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

Zadanie *Aktualizacja* musi zostać przypisane do komputerów sieci LAN organizacji, za wyjątkiem komputera, który pełni rolę źródła uaktualnień.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania i kliknij **Dalej**.

5. Zakończ działanie kreatora, klikając przycisk **Utwórz**.

Nowe zadanie zostanie wyświetlone w tabeli zadań.

6. Kliknij nowo utworzone zadanie *Aktualizacja*.

Zostanie otwarte okno właściwości zadania.

7. Przejdź do sekcji **Ustawienia aplikacji**.

8. Wybierz zakładkę **Tryb lokalny**.

9. W sekcji **Źródło aktualizacji** kliknij przycisk **Dodaj**.

10. W polu **Źródło** wprowadź ścieżkę dostępu do folderu współdzielonego.

Adres źródłowy musi odpowiadać adresowi, który wcześniej określiłeś w polu **Ścieżka**, gdy skonfigurowałeś kopiowanie pakietu aktualizacyjnego do folderu współdzielonego (patrz *powyższa instrukcja*).

11. Kliknij **OK**.

12. Skonfiguruj priorytety źródeł uaktualnień, korzystając z przycisków **W górę** i **W dół**.

13. Zapisz swoje zmiany.

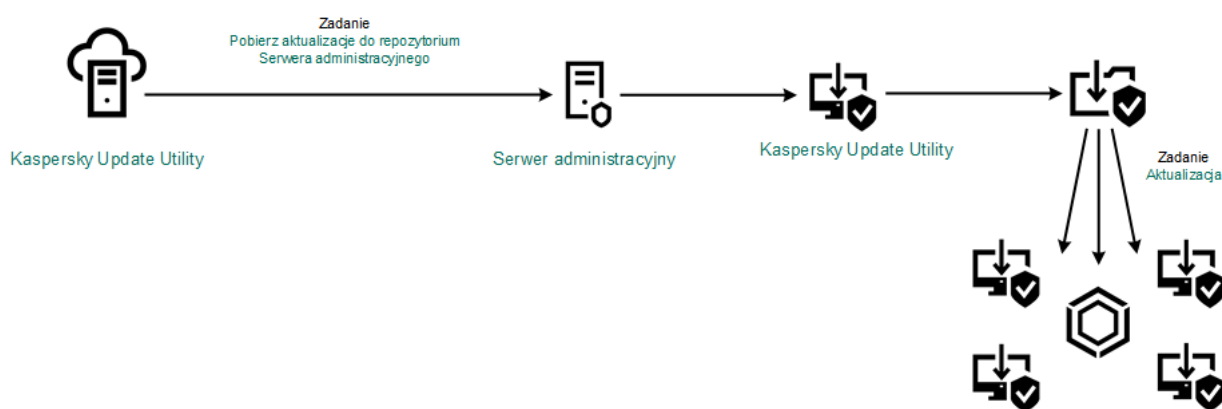
Aktualizowanie przy użyciu narzędzia Kaspersky Update Utility

Aby oszczędzić ruch sieciowy, możesz skonfigurować aktualizacje baz danych i modułów aplikacji na komputerach sieci LAN organizacji z folderu współdzielonego przy użyciu Kaspersky Update Utility. W tym celu jeden z komputerów w sieci LAN organizacji musi odbierać pakiety aktualizacji z Serwera administracyjnego Kaspersky Security Center lub z serwerów aktualizacji Kaspersky i kopiuje te pakiety aktualizacji do folderu współdzielonego przy użyciu narzędzia. Pozostałe komputery w sieci LAN organizacji będą mogły pobrać pakiety aktualizacji z tego folderu współdzielonego.

Konfigurowanie aktualizacji baz danych i modułów aplikacji z folderu współdzielonego obejmuje następujące kroki:

1. [Konfigurowanie aktualizacji baz danych i modułów aplikacji z repozytorium serwera.](#)
2. Zainstaluj narzędzie Kaspersky Update Utility na jednym z komputerów w sieci LAN organizacji.
3. Skonfiguruj kopiowanie pakietu aktualizacji do folderu współdzielonego w ustawieniach narzędzia Kaspersky Update Utility.
4. Konfigurację aktualizacji baz danych i modułów aplikacji z określonego folderu współdzielonego do pozostałych komputerów w sieci LAN organizacji.

Wersja i lokalizacja aplikacji Kaspersky Endpoint Security, która kopiuje pakiet aktualizacyjny do folderu współdzielonego, musi odpowiadać wersji i lokalizacji aplikacji, która aktualizuje bazy danych z folderu współdzielonego. Jeśli wersje lub lokalizacje aplikacji nie odpowiadają, aktualizacja baz danych może zakończyć się błędem.



Aktualizowanie przy użyciu narzędzia Kaspersky Update Utility

Możesz pobrać pakiet dystrybucyjny Kaspersky Update Utility ze [strony internetowej pomocy technicznej Kaspersky](#). Po zainstalowaniu narzędzia, wybierz źródło uaktualnień (na przykład, repozytorium Serwera administracyjnego) i folder współdzielony, do którego narzędzie Kaspersky Update Utility skopiuje pakiety aktualizacji. Szczegółowe informacje na temat korzystania z narzędzia Kaspersky Update Utility [znajdziesz w Bazie wiedzy Kaspersky](#).

W celu skonfigurowania aktualizacji z folderu współdzielonego:

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Kliknij zadanie **Aktualizacja** dla Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości zadania.
Zadanie *Aktualizacja* jest tworzone automatycznie przez Kreator wstępnej konfiguracji programu Kaspersky Security Center. Aby utworzyć zadanie *Aktualizacja*, zainstaluj wtyczkę webową Kaspersky Endpoint Security for Windows podczas działania kreatora.
3. Wybierz zakładkę **Ustawienia aplikacji** → **Tryb lokalny**.
4. Na liście źródeł uaktualnień kliknij przycisk **Dodaj**.
5. W polu **Źródło** wprowadź ścieżkę UNC do folderu współdzielonego (na przykład: \\Server\Share\Update distribution).

Adres źródłowy musi odpowiadać adresowi wskazanemu w ustawieniach Kaspersky Update Utility.

6. Kliknij **OK**.
7. Skonfiguruj priorytety źródeł uaktualnień, korzystając z przycisków **W górę** i **W dół**.
8. Zapisz swoje zmiany.

Aktualizowanie w trybie mobilnym

Tryb mobilny to tryb działania Kaspersky Endpoint Security, gdy komputer opuści sieć obwodową organizacji (*komputer offline*). Szczegółowe informacje na temat pracy z komputerami offline i użytkownikami mobilnymi *można znaleźć w [pomocy do Kaspersky Security Center](#)*.

Komputer offline poza siecią organizacji nie może nawiązać połączenia z Serwerem administracyjnym w celu zaktualizowania baz danych i modułów aplikacji. Domyślnie, tylko serwery aktualizacji Kaspersky są używane jako źródło uaktualnień do aktualizacji baz danych i modułów aplikacji w trybie mobilnym. Używanie serwera proxy do nawiązywania połączenia z internetem jest określone przez specjalny [profil użytkownika mobilnego](#). Profil użytkownika mobilnego musi zostać utworzony oddzielnie. Jeśli program Kaspersky Endpoint Security zostanie przełączony do trybu mobilnego, zadanie aktualizacji będzie uruchamiane co dwie godziny.

W celu skonfigurowania ustawień aktualizacji dla trybu mobilnego:

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Kliknij zadanie **Aktualizacja** dla Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości zadania.
Zadanie *Aktualizacja* jest tworzone automatycznie przez Kreator wstępnej konfiguracji programu Kaspersky Security Center. Aby utworzyć zadanie *Aktualizacja*, zainstaluj wtyczkę webową Kaspersky Endpoint Security for Windows podczas działania kreatora.
Wybierz zakładkę **Ustawienia aplikacji** → **Tryb mobilny**.
3. Skonfiguruj źródła uaktualnień. Źródłami uaktualnień mogą być serwery aktualizacji Kaspersky, inne serwery FTP i HTTP, foldery lokalne lub foldery sieciowe.
4. Zapisz swoje zmiany.

W wyniku tego działania, bazy danych i moduły aplikacji zostaną zaktualizowane na komputerach użytkownika, gdy przełączą się do trybu mobilnego.

Uruchamianie i zatrzymywanie zadania aktualizacji

Bez względu na wybrany tryb uruchamiania zadania aktualizacji, możesz uruchomić lub zatrzymać zadanie aktualizacji Kaspersky Endpoint Security w dowolnym momencie.

W celu uruchomienia lub zatrzymania zadania aktualizacji:

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.

2. W sekcji **Aktualizacja baz danych i modułów aplikacji** kliknij przycisk **Aktualizuj**, jeśli chcesz uruchomić zadanie aktualizacji.

Kaspersky Endpoint Security uruchomi aktualizację modułów i baz danych aplikacji. Aplikacja wyświetli postęp wykonywania zadania, rozmiar pobranych plików i źródło uaktualnień. Możesz zatrzymać zadanie w dowolnym momencie, klikając **Zatrzymaj aktualizację**.


Aby uruchomić lub zatrzymać zadanie, gdy wyświetlany jest [uproszczony interfejs aplikacji](#):

1. Kliknij prawym przyciskiem myszy ikonę aplikacji znajdującą się w obszarze powiadomień paska zadań.
2. W menu kontekstowym, z listy rozwijalnej **Zadania**:
 - wybierz nieuruchomione zadanie aktualizacji, żeby je uruchomić
 - wybierz uruchomione zadanie aktualizacji, żeby je zatrzymać
 - wybierz wstrzymane zadanie aktualizacji, żeby je wznowić lub uruchomić ponownie

Uruchamianie zadania aktualizacji z poziomu konta innego użytkownika

Domyślnie zadanie aktualizacji Kaspersky Endpoint Security jest uruchamiane z poziomu konta użytkownika, którego użyłeś do uruchomienia systemu operacyjnego. Jednakże program Kaspersky Endpoint Security może zostać zaktualizowany ze źródła uaktualnień, do którego użytkownik nie ma dostępu ze względu na brak wymaganych uprawnień (na przykład, z folderu współdzielonego, który zawiera pakiet uaktualnień) lub ze źródła uaktualnień, dla którego nie skonfigurowano autoryzacji na serwerze proxy. W ustawieniach programu Kaspersky Endpoint Security możesz wskazać użytkownika, który posiada takie uprawnienia, i skonfigurować uruchamianie aktualizacji Kaspersky Endpoint Security z poziomu konta tego użytkownika.

W celu uruchomienia zadania aktualizacji z poziomu konta innego użytkownika:


1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.
2. To spowoduje otwarcie listy zadań; wybierz zadanie aktualizacji i kliknij .
3. Kliknij **Uruchamiaj aktualizacje baz danych jako**.
4. To spowoduje otwarcie okna; w tym oknie wybierz **Inny użytkownik**.
5. Wprowadź dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami dostępu do źródła uaktualnień.
6. Zapisz swoje zmiany.

Wybieranie trybu uruchamiania zadania aktualizacji

Jeżeli z jakiegoś powodu uruchomienie zadania aktualizacji nie będzie możliwe (na przykład komputer nie będzie włączony o określonym czasie), można skonfigurować automatyczne uruchamianie pominiętego zadania przy najbliższej możliwej okazji.

Możesz odroczyć rozpoczęcie zadania po uruchomieniu aplikacji, jeżeli wybrałeś tryb uruchamiania **Zgodnie z terminarzem**, a czas włączenia Kaspersky Endpoint Security pokrywa się z czasem uruchomienia zadania aktualizacji. Zadanie aktualizacji może zostać uruchomione dopiero po minięciu określonego czasu od uruchomienia programu Kaspersky Endpoint Security.

W celu wybrania trybu uruchamiania zadania aktualizacji:

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.
2. To spowoduje otwarcie listy zadań; wybierz zadanie aktualizacji i kliknij .
3. Kliknij **Terminarz aktualizacji baz danych**.
4. W otwartym oknie wybierz tryb uruchamiania zadania aktualizacji:
 - Jeżeli Kaspersky Endpoint Security ma uruchamiać zadanie aktualizacji w zależności od tego, czy w źródle uaktualnień dostępny jest pakiet uaktualnień, wybierz **Automatycznie**. Częstotliwość sprawdzania źródła uaktualnień przez Kaspersky Endpoint Security w poszukiwaniu pakietów uaktualnień wzrasta podczas epidemii wirusów.
 - Jeżeli chcesz uruchomić aktualizację ręcznie, wybierz **Ręcznie**.
 - Jeśli chcesz skonfigurować terminarz uruchamiania zadania aktualizacji, wybierz inne opcje. Skonfiguruj zaawansowane ustawienia uruchamiania zadania aktualizacji:
 - W polu **Odrocz uruchomienie zadania po starcie aplikacji o N minut** określ czas, na jaki chcesz odroczyć uruchomienie zadania aktualizacji po uruchomieniu Kaspersky Endpoint Security.
 - Wybierz opcję **Jeśli komputer jest wyłączony, uruchom zaplanowane skanowanie następnego dnia**, jeśli chcesz, żeby Kaspersky Endpoint Security uruchomił pominięte zadania aktualizacji przy pierwszej okazji.
5. Zapisz swoje zmiany.

Dodawanie źródła uaktualnień

Źródło uaktualnień jest zasobem zawierającym uaktualnienia baz danych oraz modułów aplikacji Kaspersky Endpoint Security.


Źródłami uaktualnień mogą być serwer Kaspersky Security Center, serwery aktualizacji Kaspersky i foldery lokalne lub sieciowe.

Domyślna lista źródeł uaktualnień zawiera serwery aktualizacji Kaspersky Security Center i Kaspersky. Do listy można dodać inne źródło uaktualnień. Źródłem uaktualnień mogą być serwery HTTP/FTP oraz foldery współdzielone.

Kaspersky Endpoint Security nie obsługuje aktualizacji z serwerów HTTPS, chyba że są to serwery aktualizacji Kaspersky.

Jeżeli jako aktywne ustawiono kilka źródeł uaktualnień, Kaspersky Endpoint Security będzie podejmował próby nawiązywania połączenia z każdym z nich, poczynawszy od góry listy; uaktualnienia zostaną pobrane z pierwszego dostępnego źródła.

W celu dodania źródła uaktualnień:

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.
2. To spowoduje otwarcie listy zadań; wybierz zadanie aktualizacji i kliknij .
3. Kliknij przycisk **Wybierz źródła aktualizacji**.
4. W oknie kliknij przycisk **Dodaj**.
5. W otwartym oknie określ adres serwera FTP lub http, folderu sieciowego lub folderu lokalnego, który zawiera pakiet aktualizacyjny.

Dla źródła uaktualnień używany jest następujący format ścieżki dostępu:

- Dla serwera FTP lub HTTP wprowadź jego adres internetowy lub adres IP.
Na przykład: `http://dn1-01.geo.kaspersky.com/` lub `93.191.13.103`.
Dla serwera FTP możesz określić ustawienia autoryzacji w adresie internetowym, w następującym formacie:
`ftp://<nazwa_użytkownika>:<hasło>@<węzeł>:<port>`.
- Dla folderu sieciowego wprowadź ścieżkę UNC.
Na przykład: `\\ Server\Share\Update distribution`.
- Dla folderu lokalnego wprowadź pełną ścieżkę do tego folderu.
Na przykład: `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. Kliknij przycisk **Wybierz**.
7. Skonfiguruj priorytety źródeł uaktualnień, korzystając z przycisków **W górę** i **W dół**.
8. Zapisz swoje zmiany.

Konfigurowanie aktualizacji z foldera współdzielonego


Aby oszczędzić ruch sieciowy, możesz skonfigurować aktualizacje baz danych i modułów aplikacji na komputerach sieci LAN organizacji z folderu współdzielonego. W tym celu jeden z komputerów w sieci LAN organizacji musi odbierać pakiety aktualizacji z Serwera administracyjnego Kaspersky Security Center lub z serwerów aktualizacji Kaspersky i kopiuje go do folderu współdzielonego. Pozostałe komputery w sieci LAN organizacji będą mogły pobrać pakiety aktualizacji z tego folderu współdzielonego.

Konfigurowanie aktualizacji baz danych i modułów aplikacji z folderu współdzielonego obejmuje następujące kroki:


1. Włączenia kopiowania pakietu uaktualnień do foldera współdzielonego na jednym z komputerów w sieci lokalnej.
2. Konfigurację aktualizacji baz danych i modułów aplikacji z określonego folderu współdzielonego do pozostałych komputerów w sieci LAN organizacji.

W celu włączenia kopiowanie pakietu uaktualnień do foldera współdzielonego:

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.

2. To spowoduje otwarcie listy zadań; wybierz zadanie aktualizacji i kliknij .
3. W sekcji **Dystrybucja uaktualnień** zaznacz pole **Kopiuj aktualizacje do folderu**.
4. Wprowadź ścieżkę UNC do folderu współdzielonego (na przykład: \\Server\Share\Update distribution).
5. Zapisz swoje zmiany.



W celu skonfigurowania aktualizacji z folderu współdzielonego:

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.
2. To spowoduje otwarcie listy zadań; wybierz zadanie aktualizacji i kliknij .
3. Kliknij przycisk **Wybierz źródła aktualizacji**.
4. W oknie kliknij przycisk **Dodaj**.
5. W otwartym oknie wprowadź ścieżkę dostępu do folderu współdzielonego.

Adres źródłowy musi odpowiadać adresowi, który wcześniej określiłeś, gdy skonfigurowałeś kopiowanie pakietu aktualizacyjnego do folderu współdzielonego (patrz *powyższa instrukcja*).


6. Kliknij przycisk **Wybierz**.
7. Skonfiguruj priorytety źródeł uaktualnień, korzystając z przycisków **W górę** i **W dół**.
8. Zapisz swoje zmiany.

Aktualizowanie modułów aplikacji

Aktualizacje modułów aplikacji naprawiają błędy, udoskonalają działanie i dodają nowe funkcje. Jeśli nowe aktualizacje modułów aplikacji staną się dostępne, musisz potwierdzić instalację aktualizacji. Możesz potwierdzić instalację aktualizacji modułu aplikacji w interfejsie aplikacji lub w Kaspersky Security Center. Jeśli aktualizacja stanie się dostępna, aplikacja wyświetli jedno z następujących powiadomień w oknie głównym Kaspersky Endpoint Security: ważna aktualizacja  lub krytyczna aktualizacja . Jeśli uaktualnienia modułów aplikacji wymagają przeczytanie i zaakceptowanie warunków Umowy licencyjnej, aplikacja zainstaluje uaktualnienia po zaakceptowaniu warunków Umowy licencyjnej. Więcej informacji dotyczących śledzenia aktualizacji modułów aplikacji i potwierdzenia aktualizacji w Kaspersky Security Center można znaleźć w [pomocy do Kaspersky Security Center](#).

Po zainstalowaniu aktualizacji aplikacji konieczne może być ponowne uruchomienie komputera.

W celu skonfigurowania aktualizacji modułów aplikacji:

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.
2. To spowoduje otwarcie listy zadań; wybierz zadanie aktualizacji i kliknij .
3. W sekcji **Pobieranie i instalowanie aktualizacji modułów aplikacji** zaznacz pole **Pobierz aktualizacje składników aplikacji**.

4. Wybierz aktualizacje modułów aplikacji, które chcesz zainstalować.


- **Instaluj krytyczne i zatwierdzone aktualizacje.** Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security automatycznie instaluje krytyczne uaktualnienia, a także wszystkie inne uaktualnienia modułów aplikacji po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center.
- **Instaluj tylko zatwierdzone aktualizacje.** Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security instaluje je po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center. Ta opcja jest wybrana domyślnie.

5. Zapisz swoje zmiany.

Używanie serwera proxy do aktualizacji

Konieczne może być określenie ustawień serwera proxy do pobrania aktualizacji baz danych i modułów aplikacji ze źródła uaktualnień. Jeśli istnieje kilka źródeł uaktualnień, ustawienia serwera proxy są stosowane do wszystkich źródeł. Jeśli serwer proxy nie jest potrzebny dla niektórych źródeł uaktualnień, możesz wyłączyć korzystanie z serwera proxy we właściwościach profilu. Kaspersky Endpoint Security będzie również korzystał z serwera proxy w celu uzyskania dostępu do sieci Kaspersky Security Network i serwerów aktywacji.

W celu skonfigurowania połączenia ze źródłami uaktualnień poprzez serwer proxy:

1. W oknie głównym Web Console kliknij .
- Zostanie otwarte okno właściwości Serwera administracyjnego.
2. Przejdź do sekcji **Konfiguracja dostępu do internetu**.
3. Zaznacz pole **Użyj serwera proxy**.
4. Skonfiguruj ustawienia połączenia z serwerem proxy: adres serwera proxy, port i ustawienia uwierzytelniania (nazwa użytkownika i hasło).
5. Zapisz swoje zmiany.

W celu wyłączenia korzystania z serwera proxy dla określonej grupy administracyjnej:

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę profilu Kaspersky Endpoint Security dla komputerów, na których chcesz wyłączyć serwer proxy.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do sekcji **Ustawienia główne** → **Ustawienia sieciowe**.
5. W sekcji **Ustawienia serwera proxy** wybierz **Nie wykorzystuj serwera proxy dla adresów lokalnych**.
6. Zapisz swoje zmiany.

W celu skonfigurowania ustawień serwera proxy w interfejsie aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.

3. W sekcji **Serwer proxy** kliknij **Ustawienia serwera proxy**.

4. W otwartym oknie, w celu określenia adresu serwera proxy wybierz jedną z następujących opcji:

- **Automatycznie wykryj ustawienia serwera proxy.**

Ta opcja jest wybrana domyślnie. Kaspersky Endpoint Security używa ustawień serwera proxy, które są zdefiniowane w ustawieniach systemu operacyjnego.

- **Użyj określonych ustawień serwera proxy.**

Jeśli wybrałeś tę opcję, skonfiguruj ustawienia połączenia z serwerem proxy: port i adres serwera proxy.

5. Jeśli chcesz włączyć autoryzację na serwerze proxy, zaznacz pole **Użyj uwierzytelniania serwera proxy** i udostępni dane uwierzytelniające do swojego konta użytkownika.

6. Jeśli chcesz wyłączyć korzystanie z serwera proxy podczas [aktualizacji baz danych i modułów aplikacji](#) z folderu współdzielonego, zaznacz pole **Nie wykorzystuj serwera proxy dla adresów lokalnych**.

7. Zapisz swoje zmiany.

W rezultacie Kaspersky Endpoint Security użyje serwera proxy do pobrania aktualizacji baz danych i modułów aplikacji. Kaspersky Endpoint Security będzie również korzystał z serwera proxy w celu uzyskania dostępu do serwerów KSN i serwerów aktywacji Kaspersky. Jeśli na serwerze proxy wymagana jest autoryzacja, ale dane uwierzytelniające konta użytkownika nie zostały wprowadzone poprawnie, Kaspersky Endpoint Security wyświetli monit o podanie nazwy użytkownika i hasła.

Wycofanie ostatniej aktualizacji

Opcja cofnięcia do poprzedniej wersji baz danych i modułów staje się dostępna po pierwszej aktualizacji baz danych i modułów aplikacji.

Przy każdym uruchomieniu procesu aktualizacji program Kaspersky Endpoint Security tworzy kopię zapasową bieżących baz danych i modułów aplikacji. Umożliwi to w razie czego cofnięcie baz danych i modułów aplikacji do ich poprzedniej wersji. Funkcja cofania ostatniej aktualizacji jest przydatna w sytuacji, gdy, na przykład, nowa wersja baz danych zawiera nieprawidłową sygnaturę powodującą blokowanie bezpiecznej aplikacji.

W celu wycofania ostatniej aktualizacji:

1. W oknie głównym aplikacji przejdź do sekcji **Aktualizacja**.

2. W sekcji **Wycofywanie baz danych do ich poprzedniej wersji** kliknij przycisk **Wycofaj**.

Kaspersky Endpoint Security rozpocznie wycofywanie ostatniej aktualizacji baz danych. Aplikacja wyświetli postęp wycofywania, rozmiar pobranych plików i źródło uaktualnień. Możesz zatrzymać zadanie w dowolnym momencie, klikając **Zatrzymaj aktualizację**.

Aby uruchomić lub zatrzymać zadanie, gdy wyświetlany jest [uproszczony interfejs aplikacji](#):

1. Kliknij prawym przyciskiem myszy ikonę aplikacji znajdującą się w obszarze powiadomień paska zadań.

2. W menu kontekstowym, z listy rozwijalnej **Zadania**:

- Wybierz nieuruchomione zadanie wycofywania aktualizacji, żeby je uruchomić.

- Wybierz uruchomione zadanie wycofywania aktualizacji, żeby je zatrzymać.
- Wybierz wstrzymane zadanie wycofywania aktualizacji, żeby je wznowić lub uruchomić ponownie.

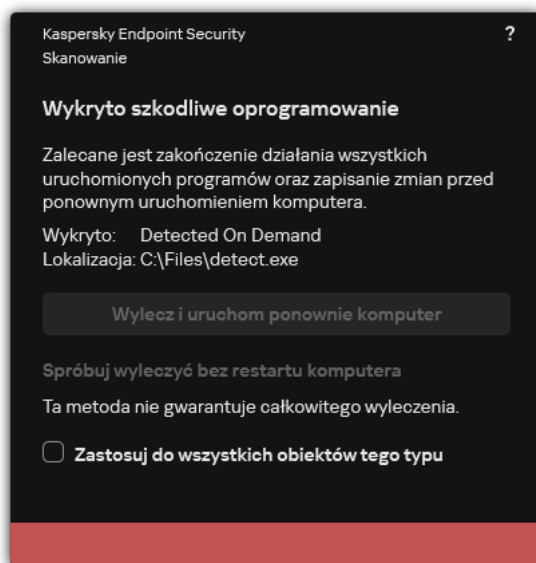
Praca z aktywnymi zagrożeniami

Kaspersky Endpoint Security zapisuje informacje o plikach, które z jakiegoś powodu nie zostały przetworzone. Informacje te są zapisywane w postaci zdarzeń na liście aktywnych zagrożeń. Aby pracować z aktywnymi zagrożeniami, Kaspersky Endpoint Security użyj technologii zaawansowanego leczenia. Zaawansowane leczenie działa inaczej dla stacji roboczych i serwerów. Możesz skonfigurować technologię zaawansowanego leczenia w [ustawieniach zadania Skanowanie antywirusowe](#) i w [ustawieniach aplikacji](#).

Leczenie aktywnych zagrożeń na stacjach roboczych

Aby pracować z aktywnymi zagrożeniami na stacjach roboczych, [włącz technologię zaawansowanego leczenia](#) w ustawieniach aplikacji. Następnie skonfiguruj doświadczenie użytkownika we właściwościach zadania [Skanowanie antywirusowe](#). We właściwościach zadania dostępne jest pole **Uruchom natychmiast Zaawansowane leczenie**. Jeśli flaga jest ustawiona, Kaspersky Endpoint Security przeprowadzi leczenie bez informowania użytkownika. Po zakończeniu leczenia, komputer zostanie uruchomiony ponownie. Jeśli flaga nie jest ustawiona, Kaspersky Endpoint Security wyświetli komunikat o aktywnych zagrożeniach (patrz rysunek poniżej). Nie możesz zamknąć tego komunikatu bez przetworzenia pliku.

Zaawansowane leczenie podczas wykonywania zadania skanowania antywirusowego na komputerze jest wykonywane tylko wtedy, gdy [funkcja Zaawansowane leczenie jest włączona](#) we właściwościach zasady zastosowanej do tego komputera.



Powiadomienie dotyczące aktywnego zagrożenia

Leczenie aktywnych zagrożeń na serwerach

W celu pracy z aktywnymi zagrożeniami na serwerach musisz:

- [włączyć technologię zaawansowanego leczenia](#) w ustawieniach aplikacji;
- [włączyć natychmiastowe zaawansowane leczenie](#) we właściwościach zadania *Skanowanie antywirusowe*.

Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows przeznaczonego dla serwerów, Kaspersky Endpoint Security nie wyświetli komunikatu. Dlatego użytkownik nie może wybrać działania wyleczenia aktywnego zagrożenia. Aby wyleczyć zagrożenie, musisz [włączyć technologię zaawansowanego leczenia](#) w ustawieniach aplikacji oraz [natychmiast włączyć Zaawansowane leczenie](#) w ustawieniach zadania *Skanowanie antywirusowe*. Następnie uruchom zadanie *Skanowanie antywirusowe*.

Przetwarzanie aktywnych zagrożeń

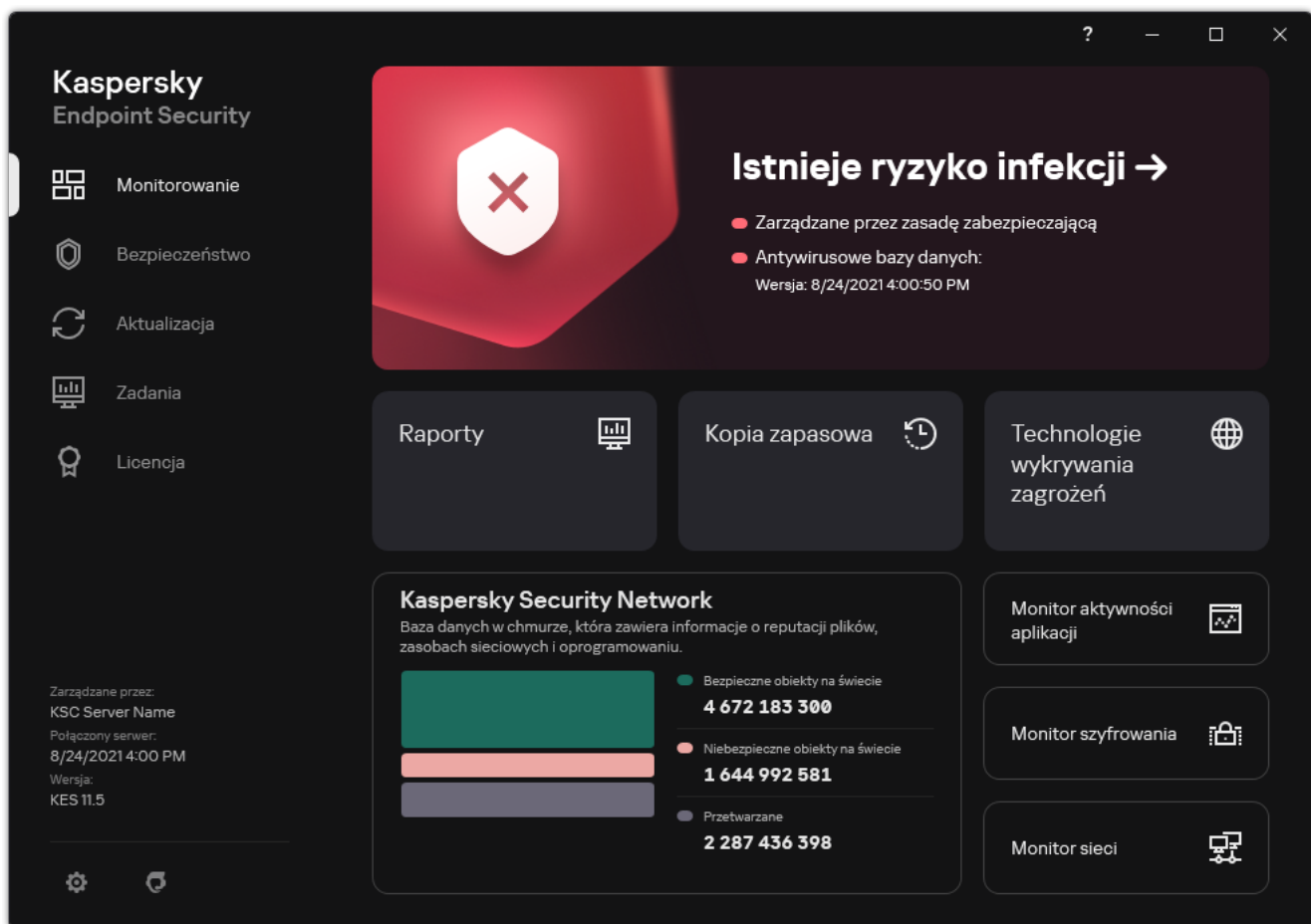
Zainfekowany plik jest uznawany za *przetworzony*, jeśli podczas skanowania w poszukiwaniu wirusów i innych zagrożeń Kaspersky Endpoint Security wykonał na nim jedną z następujących akcji określonych w ustawieniach aplikacji:

- Wykonaj leczenie.
- Usuń.
- Usuń, jeśli leczenie nie jest możliwe.

Kaspersky Endpoint Security przenosi plik na listę aktywnych zagrożeń, jeśli podczas skanowania komputera w poszukiwaniu wirusów i innych zagrożeń z jakiegoś powodu nie powiodło się wykonanie akcji na tym pliku, zgodnej z określonymi ustawieniami aplikacji.

Taka sytuacja może zajść w następujących przypadkach:

- Skanowany plik jest niedostępny (na przykład, znajduje się na dysku sieciowym lub wymiennym, do którego nie ma uprawnień zapisu).
- W sekcji **Działanie podejmowane w przypadku wykrycia zagrożenia** dla zadania skanowania wybrano opcję **Informuj**, a w oknie powiadomienia informującym o zainfekowanym pliku użytkownik wybrał opcję **Pomiń**.



Okno główne aplikacji po wykryciu zagrożenia

W celu przetworzenia aktywnych zagrożeń:

1. W oknie głównym aplikacji kliknij przycisk **Szczegóły**.
Zostanie otwarta lista aktywnych zagrożeń.
2. Wybierz obiekt, który chcesz przetworzyć.
3. Wybierz sposób zarządzania zagrożeniem:
 - **Napraw**. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki.
 - **Ignoruj**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security usunie wpis z listy aktywnych zagrożeń. Jeśli na liście nie ma aktywnych zagrożeń, stan komputera zostanie zmieniony na *OK*. Jeśli obiekt zostanie usunięty ponownie, Kaspersky Endpoint Security doda nowy wpis do listy aktywnych zagrożeń.
 - **Otwórz folder zawierający plik**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security otworzy folder zawierający obiekt w menedżerze plików. Możesz ręcznie usunąć obiekt lub przenieść obiekt do folderu, który nie znajduje się w obszarze ochrony.
 - **Dowiedz się więcej**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security otwiera [stronę internetową Encyklopedii Wirusów Kaspersky](#).

Ochrona komputera

Ochrona plików

Komponent Ochrona plików umożliwia uniknięcie infekcji systemu plików komputera. Domyślnie, składnik Ochrona plików na stałe znajduje się w pamięci RAM komputera. Składnik skanuje pliki na wszystkich dyskach komputera, a także na podłączonych dyskach. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, [usługi w chmurze Kaspersky Security Network](#) i analizy heurystycznej.


Komponent skanuje pliki otwierane przez użytkownika lub aplikację. Jeśli zostanie wykryty szkodliwy plik, Kaspersky Endpoint Security blokuje operację na pliku. Następnie aplikacja leczy lub usuwa szkodliwy plik, w zależności od ustawień komponentu Ochrona plików.

Podczas próby uzyskania dostępu do pliku, którego zawartości są przechowywane w chmurze OneDrive, Kaspersky Endpoint Security pobierze i przeskanuje zawartości plików.

Włączanie i wyłączanie modułu Ochrona plików

Domyślnie moduł Ochrona plików jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. Dla modułu Ochrona plików program Kaspersky Endpoint Security można zastosować różne grupy ustawień. Te grupy ustawień, które są zapisane w aplikacji, są nazywane *poziomami ochrony*. **Wysoki**, **Zalecany**, **Niski**. Ustawienia poziomu ochrony **Zalecany** są uważane za optymalne ustawienia zalecane przez ekspertów z Kaspersky (patrz tabela poniżej). Możesz wybrać jeden z predefiniowanych poziomów ochrony lub ręcznie skonfigurować ustawienia poziomu ochrony. Jeśli zmieniłeś ustawienia poziomu ochrony, możesz zawsze powrócić do zalecanych ustawień poziomu ochrony.

W celu włączenia lub wyłączenia komponentu Ochrona plików:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Użyj przełącznika **Ochrona plików**, aby włączyć lub wyłączyć komponent.
4. Jeśli włączyłeś komponent, w sekcji **Poziom ochrony** wykonaj jedną z następujących czynności:
 - Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony, wybierz go, korzystając z suwaka:
 - **Wysoki**. Jeśli wybrano ten poziom ochrony plików, moduł Ochrona plików będzie dokładnie kontrolować wszystkie otwierane, zapisywane i uruchamiane pliki. Komponent Ochrona plików skanuje wszystkie typy plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Moduł ten skanuje także archiwa, pakiety instalacyjne i osadzone obiekty OLE.
 - **Zalecany**. Ten poziom ochrony plików jest zalecany przez specjalistów z Kaspersky Lab. Komponent Ochrona plików skanuje wszystkie formaty plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera, a także osadzonych obiektów OLE. Moduł Ochrona plików nie skanuje archiwów oraz pakietów instalacyjnych. Wartości ustawień dla zalecanego poziomu ochrony są dostępne w poniższej tabeli.

- **Niski.** Ustawienia tego poziomu ochrony plików zapewniają maksymalną prędkość skanowania. Komponent Ochrona plików skanuje tylko pliki z określonymi rozszerzeniami na wszystkich dyskach twardej, dyskach wymiennych i dyskach sieciowych komputera. Moduł Ochrona plików nie skanuje plików złożonych.
- Jeśli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia zaawansowane** i zdefiniuj własne ustawienia komponentu.

Możesz przywrócić wartości predefiniowanych poziomów ochrony, klikając przycisk **Przywróć zalecany poziom ochrony** w górnej części okna.

5. Zapisz swoje zmiany.

Ustawienia Ochrony plików zalecane przez ekspertów z Kaspersky (zalecany poziom ochrony)

Parametr	Wartość	Opis
Typy plików	Pliki skanowane według formatu	Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował <u>tylko infekowalne pliki</u> . Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików.
Analiza heurystyczna	Niski	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.
Skanuj tylko nowe i zmienione pliki	Włączono	Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.
Technologia iSwift	Włączono	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.
Technologia iChecker	Włączono	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).
Skanuj pliki w formatach Microsoft Office	Włączono	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty.
Tryb skanowania	Tryb smart	W tym trybie Ochrona plików skanuje obiekt w oparciu o analizę akcji podejmowanych na obiekcie. Na przykład, jeżeli wykorzystywany jest


		dokument Microsoft Office, Kaspersky Endpoint Security skanuje plik przy jego pierwszym otwieraniu i ostatnim zamykaniu. Wszystkie operacje wykonywane w międzyczasie, które nadpisują plik, nie są skanowane.
Działanie podejmowane w przypadku wykrycia zagrożenia	Wylecz; usuń, jeśli leczenie nie jest możliwe	Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki.

Automatyczne wstrzymywanie Ochrony plików

Możesz skonfigurować moduł Ochrona plików tak, aby był automatycznie wstrzymywany o określonym czasie lub podczas pracy z określonymi aplikacjami.

Ochrona plików powinna zostać wstrzymana tylko w ostateczności, gdy powoduje konflikty z niektórymi aplikacjami. Jeśli podczas działania komponentu wystąpią jakiegokolwiek konflikty, zalecane jest skontaktowanie się z [pomocą techniczną Kaspersky](#). Eksperti z pomocy technicznej mogą w skonfigurowaniu komponentu Ochrona plików tak, aby mógł być uruchamiany jednocześnie z innymi aplikacjami na komputerze.

W celu skonfigurowania automatycznego wstrzymywania Ochrony plików:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. W sekcji **Wstrzymywanie modułu Ochrona plików** kliknij odnośnik **Wstrzymaj moduł Ochrona plików**.
5. W otwartym oknie skonfiguruj ustawienia wstrzymania modułu Ochrona plików:
 - a. Skonfiguruj terminarz automatycznego wstrzymania działania modułu Ochrona plików.
 - b. Utwórz listę aplikacji, których działanie powinno wstrzymać działanie modułu Ochrona plików.
6. Zapisz swoje zmiany.

Zmienianie akcji wykonywanej na zainfekowanych plikach przez moduł Ochrona plików

Domyślnie, Ochrona plików automatycznie próbuje wyleczyć wszystkie zainfekowane pliki, które zostały wykryte. Jeśli leczenie nie powiedzie się, komponent Ochrona plików usuwa te pliki.

W celu zmiany akcji wykonywanej na zainfekowanych plikach przez moduł Ochrona plików:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.

3. W sekcji **Działanie podejmowane w przypadku wykrycia zagrożenia** wybierz żądaną opcję:

- **Wylecz; usuń, jeśli leczenie nie jest możliwe.** Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki.
- **Wylecz; blokuj, jeśli leczenie nie jest możliwe.** Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie nie jest możliwe, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń.
- **Blokuj.** Jeśli wybrano tę opcję, moduł Ochrona plików automatycznie zablokuje wszystkie zainfekowane pliki, bez podjęcia próby ich wyleczenia.

Przed próbą wyleczenia lub usunięcia zainfekowanego pliku, Kaspersky Endpoint Security utworzy kopię zapasową pliku w przypadku, gdy potrzebujesz [przywrócić plik lub jeśli może zostać wyleczony w przyszłości](#).

4. Zapisz swoje zmiany.


Tworzenie obszaru ochrony modułu Ochrona plików

Obszar ochrony oznacza obiekty, które są skanowane przez moduł, gdy jest on włączony. Obszary ochrony różnych modułów mają odmienne właściwości. Lokalizacja i typ skanowanych plików to właściwości obszaru ochrony modułu Ochrona plików. Domyślnie, komponent Ochrona plików skanuje tylko [potencjalnie infekowalne pliki](#), które są uruchamiane z dysków twardej, dysków wymiennych i dysków sieciowych.

Podczas wybierania typu skanowanych plików należy pamiętać, że:

1. Istnieje małe prawdopodobieństwo wprowadzenia złośliwego kodu do plików niektórych formatów i jego późniejszej aktywacji (na przykład, formatu TXT). Istnieją jednak formaty plików zawierające kod wykonywalny (na przykład .exe, .dll). Kod wykonywalny może także znajdować się w plikach formatów, które nie są przeznaczone do tego celu (na przykład, format DOC). Ryzyko przeniknięcia i aktywacji szkodliwego kodu w takich plikach jest wysokie.
2. Cyberprzestępca może przesłać na Twój komputer wirusa lub inną szkodliwą aplikację w pliku wykonywalnym posiadającym rozszerzenie .txt. Jeśli wybierzesz opcję skanowania plików według rozszerzenia, aplikacja pominie ten plik podczas skanowania. Jeśli wybrano skanowanie plików według formatu, Kaspersky Endpoint Security analizuje nagłówek pliku niezależnie od jego rozszerzenia. Jeśli analiza wykryje, że plik posiada format pliku wykonywalnego (na przykład, EXE), aplikacja przeskanuje ten plik.

W celu utworzenia obszaru ochrony:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. W sekcji **Typy plików** określ typy plików, które mają być skanowane:

- **Wszystkie pliki.** Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia).
- **Pliki skanowane według formatu.** Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował [tylko infekowalne pliki](#). Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików.
- **Pliki skanowane według rozszerzenia.** Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował [tylko infekowalne pliki](#). Format pliku będzie określany w oparciu o jego rozszerzenie.

5. Kliknij odnośnik **Edytuj obszar ochrony**.

6. W otwartym oknie wybierz obiekty, które chcesz dodać do obszaru ochrony lub wykluczyć z niego.

Obiekty, które domyślnie znajdują się w obszarze ochrony, nie mogą zostać zmodyfikowane ani usunięte.

7. Jeśli chcesz dodać nowy obiekt do obszaru ochrony:

a. Kliknij przycisk **Dodaj**.

Zostanie otwarte drzewo folderów.

b. Wybierz obiekt i kliknij **Wybierz**.

Możesz wykluczyć obiekt ze skanowań bez usuwania go z listy obiektów w obszarze skanowania. W tym celu odznacz pole obok obiektu.


8. Zapisz swoje zmiany.

Używanie metod skanowania

Kaspersky Endpoint Security używa techniki skanowania nazywanej *Uczenie maszynowe* oraz analizy przy użyciu sygnatur. Podczas analizy sygnatur Kaspersky Endpoint Security porównuje wykryty obiekt z wpisami w swojej bazie danych. W oparciu o zalecenia ekspertów z Kaspersky, uczenie maszynowe i analiza sygnatur jest zawsze włączona.

Aby zwiększyć efektywność ochrony, możesz użyć analizy heurystycznej. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.

W celu skonfigurowania użycia analizy heurystycznej w działaniu modułu Ochrona plików:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij przycisk **Ustawienia zaawansowane**.

4. Jeśli chcesz, żeby aplikacja korzystała z analizy heurystycznej do ochrony przed zagrożeniami plikowymi, w sekcji **Metody skanowania** zaznacz pole **Analiza heurystyczna**. Następnie użyj suwaka, aby ustawić poziom analizy heurystycznej: **Niski**, **Średni** lub **Szczegółowy**.

5. Zapisz swoje zmiany.

Używanie technologii skanowania w działaniu modułu Ochrona plików

W celu skonfigurowania korzystania z technologii skanowania w trakcie działania Ochrony plików:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. W sekcji **Technologie skanowania** zaznacz pola obok nazw technologii, której chcesz użyć do ochrony przed zagrożeniami plikowymi:
 - **Technologia iSwift**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.
 - **Technologia iChecker**. Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).


5. Zapisz swoje zmiany.

Optymalizowanie skanowania plików

Możesz zoptymalizować skanowanie plików, zmniejszając czas skanowania i zwiększając szybkość działania programu Kaspersky Endpoint Security. Można to uzyskać poprzez skanowanie tylko nowych plików i tych plików, które zostały zmodyfikowane od ostatniego skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.

Możesz także [włączyć korzystanie z technologii iChecker i iSwift](#), co zoptymalizuje prędkość skanowania plików poprzez wykluczenie plików, które nie zostały zmodyfikowane od ostatniego skanowania.

W celu zoptymalizowania skanowania plików:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij przycisk **Ustawienia zaawansowane**.

4. W sekcji **Optymalizacja skanowania** zaznacz pole **Skanuj tylko nowe i zmienione pliki**.

5. Zapisz swoje zmiany.


Skanowanie plików złożonych

Popularną techniką ukrywania wirusów i innego szkodliwego oprogramowania jest osadzanie ich w plikach złożonych, takich jak archiwa czy bazy danych. W celu wykrycia ukrytych w ten sposób wirusów i innego szkodliwego oprogramowania, plik złożony musi zostać rozpakowany, co może spowolnić skanowanie. Możesz ograniczyć typy skanowanych plików złożonych, dzięki czemu skanowanie będzie szybsze.

Metoda używana do przetwarzania zainfekowanego pliku złożonego (leczenie lub usuwanie) zależy od typu pliku.

Ochrona plików wyleczy pliki złożone w formatach RAR, ARJ, ZIP, CAB i LHA i usunie pliki we wszystkich pozostałych formatach (za wyjątkiem pocztowych baz danych).

W celu skonfigurowania skanowania plików złożonych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. W sekcji **Skanowanie plików złożonych** określ, które pliki złożone mają być skanowane: archiwa, pakiety instalacyjne lub pliki w formatach pakietu Office.
5. Jeśli [skanowanie tylko nowych i zmodyfikowanych plików zostało wyłączone](#), skonfiguruj ustawienia każdego typu pliku złożonego: skanuj wszystkie pliki tego typu lub tylko nowe pliki.
Jeśli skanowanie tylko nowych i zmodyfikowanych plików zostało włączone, Kaspersky Endpoint Security skanuje tylko nowe i zmodyfikowane pliki wszystkich typów plików złożonych.
6. Skonfiguruj zaawansowane ustawienia skanowania plików złożonych.

- **Nie rozpakowuj dużych plików złożonych.**

Jeżeli to pole jest zaznaczone, Kaspersky Endpoint Security nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość.

Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki złożone o wszystkich rozmiarach.

Kaspersky Endpoint Security skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

- **Rozpakowywanie plików złożonych w tle.**

Jeśli pole jest zaznaczone, Kaspersky Endpoint Security oferuje dostęp do plików złożonych, które mają większy rozmiar niż wartość określona przed skanowaniem tych plików. W tym przypadku Kaspersky Endpoint Security rozpakowuje i skanuje pliki złożone w tle.

Kaspersky Endpoint Security oferuje dostęp do plików złożonych, których rozmiar jest mniejszy niż ta wartość dopiero po rozpakowaniu i przeskanowaniu tych plików.


Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security oferuje dostęp do plików złożonych dopiero po rozpakowaniu i przeskanowaniu plików dowolnego rozmiaru.

7. Zapisz swoje zmiany.

Zmianie trybu skanowania

Tryb skanowania odnosi się do warunku wyzwającego skanowanie pliku przez moduł Ochrona plików. Domyślnie program Kaspersky Endpoint Security skanuje pliki w trybie smart. W tym trybie skanowania Ochrona plików decyduje czy skanować pliki po przeanalizowaniu operacji wykonywanych na pliku przez użytkownika, aplikację w imieniu użytkownika (z poziomu konta, które zostało użyte przy logowaniu lub z poziomu innego konta użytkownika), bądź przez system operacyjny. Na przykład, jeżeli wykorzystywany jest dokument programu Microsoft Office Word, aplikacja skanuje plik przy jego pierwszym otwieraniu i ostatnim zamykaniu. Wszystkie operacje wykonywane w międzyczasie, które nadpisują plik, nie są skanowane.

W celu zmiany trybu skanowania plików:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona plików**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. W sekcji **Tryb skanowania** wybierz żądany tryb:
 - **Tryb smart.** W tym trybie Ochrona plików skanuje obiekt w oparciu o analizę akcji podejmowanych na obiekcie. Na przykład, jeżeli wykorzystywany jest dokument Microsoft Office, Kaspersky Endpoint Security skanuje plik przy jego pierwszym otwieraniu i ostatnim zamykaniu. Wszystkie operacje wykonywane w międzyczasie, które nadpisują plik, nie są skanowane.
 - **Podczas dostępu i modyfikacji.** W tym trybie moduł Ochrona plików skanuje obiekty za każdym razem, gdy są otwierane lub modyfikowane.
 - **Podczas dostępu.** W tym trybie moduł Ochrona plików skanuje obiekty podczas ich otwierania.
 - **Podczas wykonywania.** W tym trybie moduł Ochrona plików skanuje obiekty jedynie podczas ich uruchamiania.
5. Zapisz swoje zmiany.

Ochrona WWW

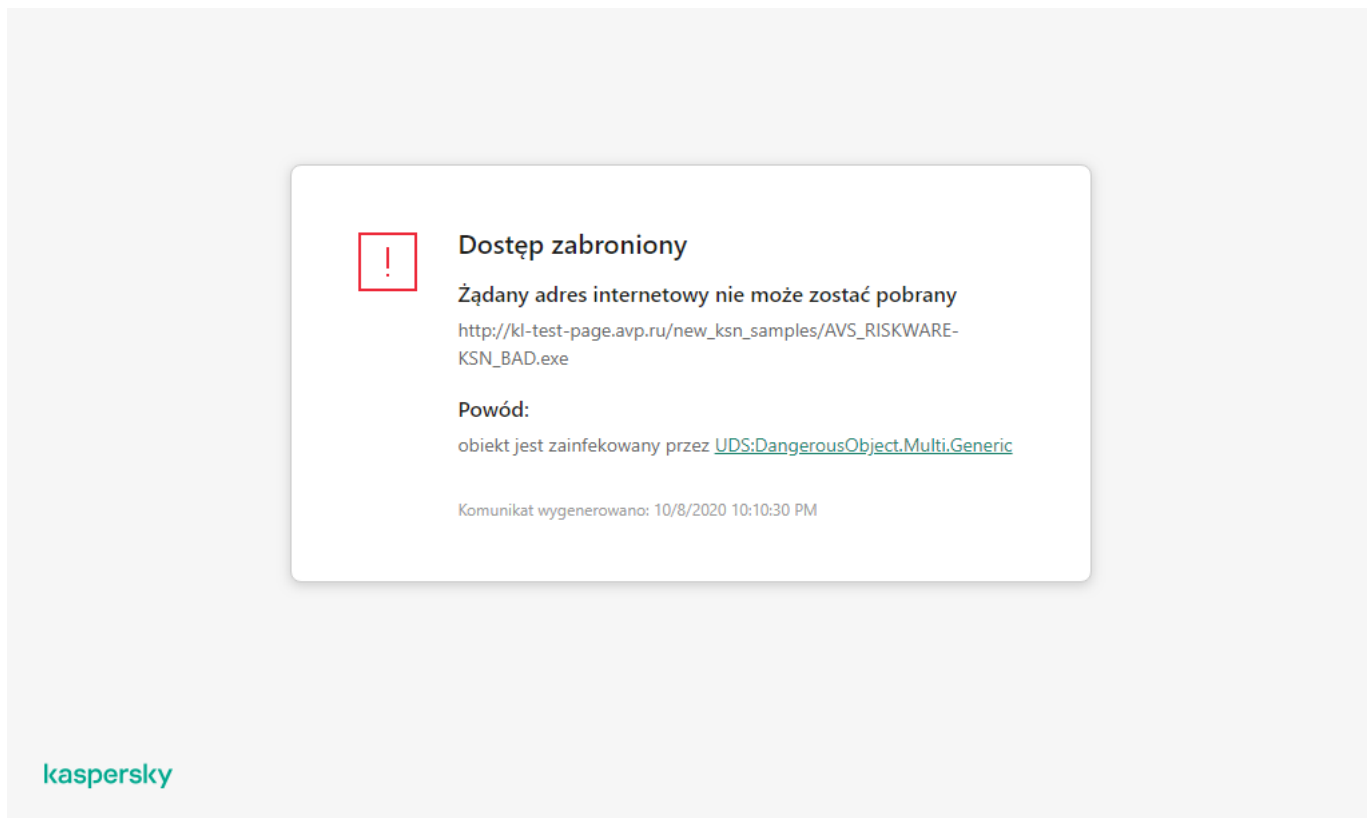
Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Komponent Ochrona WWW zapobiega pobieraniu szkodliwych plików z internetu, a także blokuje szkodliwe i phishingowe strony internetowe. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, [usługi w chmurze Kaspersky Security Network](#) i analizy heurystycznej.

Kaspersky Endpoint Security skanuje ruch HTTP, HTTPS i FTP. Kaspersky Endpoint Security skanuje adresy internetowe i adresy IP. Możesz [określić porty monitorowane przez Kaspersky Endpoint Security](#), lub wybrać wszystkie porty.

Dla monitorowania ruchu HTTPS należy [włączyć skanowanie zaszyfrowanych połączeń](#).

Gdy użytkownik próbuje otworzyć złośliwą lub phishingową stronę internetową, Kaspersky Endpoint Security zablokuje dostęp i wyświetli ostrzeżenie (patrz rysunek poniżej).



Wiadomość o odmowie dostępu do strony internetowej

Włączanie i wyłączanie modułu Ochrona WWW

Domyślnie moduł Ochrona WWW jest włączony i działa w trybie zalecany przez ekspertów z Kaspersky. Dla modułu Ochrona WWW program Kaspersky Endpoint Security można zastosować różne grupy ustawień. Te grupy ustawień, które są zapisane w aplikacji, są nazywane *poziomami ochrony*. **Wysoki, Zalecany, Niski**. Ustawienia **Zalecanego** poziomu ochrony ruchu sieciowego są uważane za optymalne ustawienia zalecane przez ekspertów z Kaspersky (patrz poniższa tabela). Możesz wybrać jeden z predefiniowanych poziomów ochrony ruchu sieciowego, odbieranego lub wysyłanego przez protokoły HTTP i FTP, lub skonfigurować niestandardowy poziom ochrony ruchu sieciowego. Jeśli zmienisz ustawienia poziomu ochrony ruchu sieciowego, możesz zawsze powrócić do zalecanych ustawień poziomu ochrony.

W celu włączenia lub wyłączenia komponentu Ochrona WWW:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.

3. Użyj przełącznika **Ochrona WWW**, aby włączyć lub wyłączyć komponent.

4. Jeśli włączyłeś komponent, w sekcji **Poziom ochrony** wykonaj jedną z następujących czynności:

- Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony, wybierz go, korzystając z suwaka:
 - **Wysoki.** Poziom ochrony, zgodnie z którym Ochrona WWW przeprowadza skanowanie ruchu sieciowego, odbieranego przez komputer poprzez protokoły HTTP i FTP, na maksymalnym poziomie. Ochrona WWW szczegółowo skanuje wszystkie obiekty ruchu sieciowego, używając pełnego zestawu baz danych aplikacji, a także przeprowadza najbardziej szczegółową [analizę heurystyczną](#).
 - **Zalecany.** Jest to poziom ochrony zapewniający optymalną równowagę pomiędzy wydajnością Kaspersky Endpoint Security a ochroną ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na **średnim** poziomie. Ten poziom ochrony ruchu sieciowego jest zalecany przez specjalistów z Kaspersky. Wartości ustawień dla zalecanego poziomu ochrony są dostępne w poniższej tabeli.
 - **Niski.** Ustawienia tego poziomu ochrony ruchu sieciowego zapewniają maksymalną prędkość skanowania ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na **niskim** poziomie.
- Jeśli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia zaawansowane** i zdefiniuj własne ustawienia komponentu.

Możesz przywrócić wartości predefiniowanych poziomów ochrony, klikając przycisk **Przywróć zalecany poziom ochrony** w górnej części okna.

5. Zapisz swoje zmiany.

Ustawienia Ochrony WWW zalecane przez ekspertów z Kaspersky (zalecany poziom ochrony)


Parametr	Wartość	Opis
Sprawdź adres internetowy zgodnie z bazą szkodliwych adresów internetowych	Włączono	Skanowanie odnośników do określenia, czy znajdują się w bazie danych szkodliwych odnośników pozwoli na śledzenie stron internetowych, które zostały dodane do listy zablokowanych. Baza danych szkodliwych adresów internetowych, która została stworzona przez Kaspersky, znajduje się w pakiecie instalacyjnym aplikacji i jest aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.
Sprawdź adres internetowy zgodnie z bazą phishingowych adresów internetowych	Włączono	Baza danych phishingowych adresów internetowych zawiera adresy internetowe obecnie znanych stron wykorzystywanych przy atakach phishingowych. Kaspersky uzupełnia tę bazę odnośników phishingowych o adresy uzyskane z międzynarodowej organizacji znanej jako Anti-Phishing Working Group. Baza danych adresów phishingowych znajduje się w pakiecie instalacyjnym aplikacji, jest również aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.
Użyj analizy heurystycznej (Ochrona WWW)	Średni	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Jeśli ruch sieciowy jest skanowany w poszukiwaniu wirusów i innych aplikacji, które stwarzają zagrożenie, analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.

Użyj analizy heurystycznej (Anti-Phishing)	Włączono	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa.
Działanie podejmowane w przypadku wykrycia zagrożenia	Zablokuj pobranie	Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Ochrona WWW zablokuje dostęp do obiektu i wyświetli komunikat w przeglądarce.

Zmianie akcji podejmowanej na szkodliwych obiektach w ruchu sieciowym

Domyślnie, po wykryciu zainfekowanego obiektu w ruchu sieciowym, Ochrona WWW zablokuje dostęp do obiektu i wyświetli komunikat o podjętym działaniu.

W celu zmiany akcji podejmowanej na szkodliwych obiektach w ruchu sieciowym:


1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
3. W sekcji **Działanie podejmowane w przypadku wykrycia zagrożenia** wybierz wymaganą akcję, wykonywaną przez Kaspersky Endpoint Security po wykryciu szkodliwego obiektu w ruchu sieciowym:
 - **Zablokuj pobranie.** Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Ochrona WWW zablokuje dostęp do obiektu i wyświetli komunikat w przeglądarce.
 - **Informuj.** Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Kaspersky Endpoint Security pozwala na pobranie tego obiektu na komputer, ale dodaje informacje o zainfekowanym obiekcie do listy aktywnych zagrożeń.
4. Zapisz swoje zmiany.

Skanowanie adresów internetowych z wykorzystaniem baz danych phishingowych i szkodliwych adresów internetowych

Skanowanie odnośników w celu sprawdzenia, czy znajdują się na liście phishingowych adresów internetowych pozwala na uniknięcie *ataków phishingowych*. Atak phishingowy może być zamaskowany, na przykład, pod postacią wiadomości e-mail od banku z odsyłaczem do oficjalnej strony WWW banku. Po kliknięciu odnośnika zostaje otwarta strona internetowa przypominająca tę należącą do danej instytucji finansowej. W rzeczywistości jednak znajdziesz się na spreparowanej stronie. Od tego momentu wszystkie Twoje działania są śledzone i mogą zostać użyte do kradzieży pieniędzy.

Odnośniki do stron typu phishing mogą być otrzymywane zarówno za pomocą poczty elektronicznej, jak również z innych zasobów, takich jak wiadomości ICQ. Z tego powodu moduł Ochrona WWW monitoruje próby dostępu do stron phishingowych na poziomie ruchu sieciowego oraz blokuje dostęp do takich stron. Lista adresów phishingowych znajduje się w pakiecie dystrybucyjnym programu Kaspersky Endpoint Security.

W celu skonfigurowania modułu Ochrona WWW, aby sprawdzał, czy odnośniki znajdują się w bazie danych szkodliwych adresów i adresów typu phishing:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. Wykonaj następujące czynności:
 - Jeśli chcesz, aby Ochrona WWW sprawdzała odnośniki w bazach danych szkodliwych adresów internetowych, zaznacz pole **Sprawdź adres internetowy zgodnie z bazą szkodliwych adresów internetowych** w sekcji **Metody skanowania**. Skanowanie odnośników do określenia, czy znajdują się w bazie danych szkodliwych odnośników pozwoli na śledzenie stron internetowych, które zostały dodane do listy zablokowanych. Baza danych szkodliwych adresów internetowych, która została stworzona przez Kaspersky, znajduje się w pakiecie instalacyjnym aplikacji i jest aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.

Kaspersky Endpoint skanuje wszystkie odnośniki, aby określić, czy znajdują się w bazie danych szkodliwych adresów internetowych. Ustawienia skanowania bezpiecznego połączenia aplikacji nie wpływają na funkcjonalność skanowania odnośników. Innymi słowy, jeśli [skanowanie połączeń szyfrowanych jest wyłączone](#), Kaspersky Endpoint Security sprawdza odnośniki w bazach danych szkodliwych adresów internetowych nawet wtedy, gdy ruch sieciowy jest przesyłany poprzez połączenie szyfrowane.

- Jeśli chcesz, żeby komponent Ochrona WWW sprawdzał odnośniki w bazach danych phishingowych adresów internetowych, w sekcji **Anti-Phishing** zaznacz pole **Sprawdź adres internetowy zgodnie z bazą phishingowych adresów internetowych**. Baza danych phishingowych adresów internetowych zawiera adresy internetowe obecnie znanych stron wykorzystywanych przy atakach phishingowych. Kaspersky uzupełnia tę bazę odnośników phishingowych o adresy uzyskane z międzynarodowej organizacji znanej jako Anti-Phishing Working Group. Baza danych adresów phishingowych znajduje się w pakiecie instalacyjnym aplikacji, jest również aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.


Możesz również sprawdzać odnośniki, korzystając z baz danych reputacji pochodzących z [Kaspersky Security Network](#).

5. Zapisz swoje zmiany.

Używanie analizy heurystycznej w działaniu modułu Ochrona WWW

Aby zwiększyć efektywność ochrony, możesz użyć analizy heurystycznej. Podczas analizy heurystycznej Kaspersky Endpoint Security analizuje aktywność aplikacji w systemie operacyjnym. Analiza heurystyczna może wykryć zagrożenia, dla których nie ma wpisów w bazach danych Kaspersky Endpoint Security.

W celu skonfigurowania korzystania z analizy heurystycznej:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia zaawansowane**.


4. W sekcji **Metody skanowania** zaznacz pole **Użyj analizy heurystycznej**, jeśli chcesz, żeby aplikacja używała analizy heurystycznej podczas skanowania ruchu sieciowego pod kątem wirusów i innych szkodliwych programów. Następnie użyj suwaka, aby ustawić poziom analizy heurystycznej: **Niski**, **Średni** lub **Szczegółowy**.
5. W sekcji **Anti-Phishing** zaznacz pole **Użyj analizy heurystycznej**, jeśli chcesz, żeby aplikacja używała analizy heurystycznej podczas skanowania stron internetowych pod kątem odnośników phishingowych.
6. Zapisz swoje zmiany.

Tworzenie listy zaufanych adresów internetowych

Możesz utworzyć listę adresów internetowych, którym ufasz co do zawartości. Ochrona WWW nie sprawdza informacji pochodzących od zaufanych adresów internetowych w poszukiwaniu wirusów i innych zagrożeń. Ta opcja może być użyteczna, na przykład, gdy moduł nie pozwala na pobranie pliku ze znanej strony internetowej.

Adres internetowy może być adresem konkretnej strony internetowej lub witryny.

W celu utworzenia listy zaufanych adresów internetowych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. Zaznacz pole **Nie skanuj ruchu sieciowego z zaufanych adresów internetowych**.
Jeśli pole jest zaznaczone, moduł Ochrona WWW nie skanuje zawartości stron internetowych, których adresy znajdują się na liście zaufanych adresów internetowych. Do listy zaufanych adresów internetowych możesz dodać określony adres i maskę adresu strony internetowej.
5. Utwórz listę adresów internetowych / stron internetowych, którym ufasz co do zawartości.
6. Zapisz swoje zmiany.

Eksportowanie i importowanie listy zaufanych adresów internetowych

Możesz wyeksportować listę zaufanych adresów internetowych do pliku XML. Następnie możesz zmodyfikować plik, na przykład, dodać dużą liczbę adresów internetowych tego samego typu. Możesz także użyć funkcji eksportowania/importowania w celu utworzenia kopii zapasowej listy zaufanych adresów internetowych lub w celu przeniesienia listy na inny serwer.

[Eksportowanie i importowanie listy zaufanych adresów sieciowych w Konsoli administracyjnej.\(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
6. Kliknij przycisk **Ustawienia**.
7. W otwartym oknie wybierz zakładkę **Zaufane adresy internetowe**.
8. W celu utworzenia listy zaufanych adresów internetowych:
 - a. Wybierz zaufane adresy internetowe, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

Jeśli nie wybrałeś żadnego zaufanego adresu internetowego, Kaspersky Endpoint Security wyeksportuje wszystkie adresy internetowe.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę zaufanych adresów internetowych, wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.

Kaspersky Endpoint Security wyeksportuje całą listę zaufanych adresów internetowych do pliku XML.
9. W celu zaimportowania listy zaufanych adresów:
 - a. Kliknij odnośnik **Importuj**.

W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę zaufanych adresów.
 - b. Kliknij przycisk **Otwórz**.

Jeśli komputer ma już listę zaufanych adresów, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
10. Zapisz swoje zmiany.

[Eksportowanie i importowanie listy zaufanych adresów internetowych w Web Console i Cloud Console](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listę zaufanych adresów internetowych.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona WWW**.
5. W celu wyeksportowania listy wykluczeń w sekcji **Zaufane adresy internetowe**:
 - a. Wybierz zaufane adresy internetowe, które chcesz wyeksportować.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę zaufanych adresów internetowych, wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security wyeksportuje całą listę zaufanych adresów internetowych do pliku XML.
6. W celu zaimportowania listy wykluczeń w sekcji **Zaufane adresy internetowe**:
 - a. Kliknij odnośnik **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę zaufanych adresów.
 - b. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę zaufanych adresów, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
7. Zapisz swoje zmiany.

Ochrona poczty

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Ochrona poczty skanuje załączniki odbieranych i wysyłanych wiadomości e-mail w poszukiwaniu wirusów i innych zagrożeń. Komponent skanuje również wiadomości w poszukiwaniu szkodliwych i phishingowych odnośników. Domyślnie, składnik Ochrona poczty na stałe znajduje się w pamięci RAM komputera i skanuje wszystkie wiadomości otrzymane lub wysłane za pomocą protokołów POP3, SMTP, IMAP lub NNTP lub klienta poczty Microsoft Office Outlook (MAPI). Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, [usługi w chmurze Kaspersky Security Network](#) i analizy heurystycznej.

Komponent Ochrona poczty nie skanuje wiadomości, jeśli klient poczty jest otwarty w przeglądarce.


Jeśli w załączniku zostanie wykryty szkodliwy plik, Kaspersky Endpoint Security zmieni nazwę tematu wiadomości w następujący sposób: [Wiadomość jest zainfekowana] <temat wiadomości> lub [Usunięto zainfekowany obiekt] <temat wiadomości>.

Składnik współdziała z klientami poczty e-mail zainstalowanymi na komputerze. W przypadku klienta poczty Microsoft Office Outlook dostarczane jest [rozszerzenie z dodatkowymi parametrami](#). Rozszerzenie Ochrony poczty jest integrowane z programem pocztowym Microsoft Office Outlook w trakcie instalacji Kaspersky Endpoint Security.

Włączanie i wyłączanie modułu Ochrona poczty

Domyślnie moduł Ochrona poczty jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. Dla modułu Ochrona poczty program Kaspersky Endpoint Security stosuje różne grupy ustawień. Te grupy ustawień, które są zapisane w aplikacji, są nazywane *poziomami ochrony*: **Wysoki**, **Zalecany**, **Niski**. Ustawienia **Zalecanego** poziomu ochrony poczty są uważane za optymalne ustawienia zalecane przez ekspertów z Kaspersky (patrz poniższa tabela). Możesz wybrać jeden z predefiniowanych poziomów ochrony poczty lub skonfigurować niestandardowy poziom ochrony poczty. Jeśli zmienisz ustawienia poziomu ochrony poczty, możesz zawsze powrócić do zalecanych ustawień poziomu ochrony poczty.

W celu włączenia lub wyłączenia komponentu Ochrona poczty:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
3. Użyj przełącznika **Ochrona poczty**, aby włączyć lub wyłączyć komponent.
4. Jeśli włączyłeś komponent, w sekcji **Poziom ochrony** wykonaj jedną z następujących czynności:
 - Jeśli chcesz zastosować jeden z predefiniowanych poziomów ochrony, wybierz go, korzystając z suwaka:
 - **Wysoki**. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty szczegółowo skanuje wiadomości e-mail. Ochrona poczty skanuje przychodzące i wychodzące wiadomości e-mail, a także przeprowadza szczegółową analizę heurystyczną. **Wysoki** poziom ochrony poczty jest zalecany dla środowisk wysokiego ryzyka. Przykładem takiego środowiska jest korzystanie z darmowego serwera pocztowego, który nie jest chroniony żadnym systemem antywirusowym.
 - **Zalecany**. Jest to poziom ochrony zapewniający optymalną równowagę pomiędzy wydajnością Kaspersky Endpoint Security a ochroną poczty. Ochrona poczty skanuje wiadomości przychodzące i wychodzące, a także przeprowadza analizę heurystyczną na średnim poziomie intensywności. Ten poziom ochrony ruchu pocztowego jest zalecany przez specjalistów z Kaspersky. Wartości ustawień dla zalecanego poziomu ochrony są dostępne w poniższej tabeli.
 - **Niski**. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty skanuje tylko wiadomości przychodzące, wykonuje analizę heurystyczną na niskim poziomie, a także nie skanuje archiwów załączonych do wiadomości e-mail. Na tym poziomie moduł Ochrona poczty skanuje wiadomości z maksymalną prędkością i używa minimalnej ilości zasobów systemu operacyjnego. **Niski** poziom ochrony jest zalecany podczas pracy w dobrze chronionym środowisku. Przykładem takiego środowiska może być firmowa sieć LAN ze scentralizowaną ochroną poczty.

- Jeśli chcesz skonfigurować niestandardowy poziom ochrony, kliknij przycisk **Ustawienia zaawansowane** i zdefiniuj własne ustawienia komponentu.

Możesz przywrócić wartości predefiniowanych poziomów ochrony, klikając przycisk **Przywróć zalecany poziom ochrony** w górnej części okna.

5. Zapisz swoje zmiany.

Ustawienia Ochrony poczty zalecane przez ekspertów z Kaspersky (zalecany poziom ochrony)


Parametr	Wartość	Opis
Obszar ochrony	Wiadomości odbierane i wysyłane	<i>Obszar ochrony</i> obejmuje obiekty, które komponent sprawdza podczas działania: Wiadomości odbierane i wysyłane lub Tylko wiadomości przychodzące . Aby chronić komputery, należy skanować tylko wiadomości przychodzące. Możesz włączyć skanowanie wiadomości wychodzących, aby zapobiec wysłaniu zainfekowanych plików w archiwach. Możesz także włączyć skanowanie wiadomości wychodzących, jeśli chcesz zapobiec wysłaniu plików w określonych formatach, na przykład plików audio i wideo.
Włącz rozszerzenie Microsoft Outlook	Włączono	Jeśli pole jest zaznaczone, skanowanie wiadomości przesyłanych poprzez protokoły POP3, SMTP, NNTP, IMAP jest włączone po stronie rozszerzenia zintegrowanego w Microsoft Outlook. Jeśli poczta jest skanowana przy użyciu rozszerzenia dla programu Microsoft Outlook, zalecane jest korzystanie z trybu buforowanego programu Exchange. Więcej informacji dotyczących trybu buforowanego programu Exchange oraz zalecenia dotyczące korzystania z tego trybu można znaleźć w Bazie wiedzy Microsoft .
Skanuj załączone archiwa	Włączono	Skanuje archiwa w następujących formatach: RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
Skanuj załączone pliki formatów pakietu Office	Włączono	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty.
Filtr załączników	Zmień nazwy załączników określonych typów	Jeśli wybierzesz tę opcję, Ochrona poczty zastąpi ostatni znak rozszerzenia wykryty w załączonych plikach określonych typów znakiem podkreślenia (na przykład: attachment.doc_). Dlatego, aby otworzyć plik, użytkownik musi zmienić jego nazwę.
Analiza heurystyczna	Średni	Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa. Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.
Działanie	Wylecz;	Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej

podejmowane w przypadku wykrycia zagrożenia	usuń, jeśli leczenie nie jest możliwe	lub wychodzącej, Kaspersky Endpoint Security podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, Kaspersky Endpoint Security usunie zainfekowany obiekt. Kaspersky Endpoint Security dodaje do tematu wiadomości informacje o wykonanym działaniu: [Usunięto zainfekowany obiekt] <temat wiadomości>.
---	---------------------------------------	--

Zmianie akcji podejmowanej na zainfekowanych wiadomościach e-mail

Domyślnie, Ochrona poczty automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych wiadomości, które zostały wykryte. Jeśli leczenie nie powiedzie się, komponent Ochrona poczty usuwa zainfekowane wiadomości e-mail.


W celu zmiany akcji podejmowanej na zainfekowanych wiadomościach e-mail:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
3. W sekcji **Działanie podejmowane w przypadku wykrycia zagrożenia** wybierz akcję, jaką Kaspersky Endpoint Security wykona po wykryciu zainfekowanej wiadomości:
 - **Wylecz; usuń, jeśli leczenie nie jest możliwe.** Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej lub wychodzącej, Kaspersky Endpoint Security podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, Kaspersky Endpoint Security usunie zainfekowany obiekt. Kaspersky Endpoint Security dodaje do tematu wiadomości informacje o wykonanym działaniu: [Usunięto zainfekowany obiekt] <temat wiadomości>.
 - **Wylecz; blokuj, jeśli leczenie nie jest możliwe.** Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, Kaspersky Endpoint Security podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, Kaspersky Endpoint Security doda ostrzeżenie do tematu wiadomości: [Wiadomość zainfekowana] <temat wiadomości>. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, Kaspersky Endpoint Security podejmie próbę wyleczenia wykrytego obiektu. Jeśli obiektu nie można wyleczyć, Kaspersky Endpoint Security zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.
 - **Blokuj.** Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, Kaspersky Endpoint Security doda ostrzeżenie do tematu wiadomości: [Wiadomość zainfekowana] <temat wiadomości>. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, Kaspersky Endpoint Security zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.
4. Zapisz swoje zmiany.

Tworzenie obszaru ochrony modułu Ochrona poczty

Obszar ochrony odnosi się do obiektów, które są skanowane przez komponent, gdy jest on aktywny. Obszary ochrony różnych modułów mają odmienne właściwości. Właściwości obszaru ochrony modułu Ochrona poczty zawierają ustawienia integracji Ochrony poczty z klientami poczty oraz typy wiadomości pocztowych i protokołów pocztowych, których ruch jest skanowany przez Ochronę poczty. Domyślnie, Kaspersky Endpoint Security skanuje przychodzące i wychodzące wiadomości pocztowe oraz ruch przesyłany przez protokoły POP3, SMTP, NNTP i IMAP, integruje się również z klientem poczty Microsoft Office Outlook.

W celu utworzenia obszaru ochrony modułu Ochrona poczty:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. W sekcji **Obszar ochrony** wybierz wiadomości, które będą skanowane:

- **Wiadomości odbierane i wysyłane.**
- **Tylko przychodzące.**

Aby chronić komputery, należy skanować tylko wiadomości przychodzące. Możesz włączyć skanowanie wiadomości wychodzących, aby zapobiec wysłaniu zainfekowanych plików w archiwach. Możesz także włączyć skanowanie wiadomości wychodzących, jeśli chcesz zapobiec wysłaniu plików w określonych formatach, na przykład plików audio i wideo.

Jeśli wybierzesz opcję skanowania tylko wiadomości odbieranych, zalecane jest przeprowadzenie jednorazowego skanowania wszystkich wiadomości wychodzących, aby sprawdzić, czy na Twoim komputerze nie ma robaków pocztowych, rozpowszechnianych za pośrednictwem wiadomości e-mail. Pozwoli to uniknąć problemów wynikających z niekontrolowanego wysyłania masowych, zainfekowanych wiadomości z Twojego komputera.

5. W sekcji **Łączność** wykonaj następujące czynności:

- Jeśli chcesz, aby Ochrona poczty skanowała wiadomości pocztowe przesyłane poprzez protokoły POP3, SMTP, NNTP i IMAP zanim dotrą one na komputer użytkownika, zaznacz pole **Skanuj ruch POP3, SMTP, NNTP i IMAP**.

Jeśli nie chcesz, aby Ochrona poczty skanowała wiadomości pocztowe przesyłane poprzez protokoły POP3, SMTP, NNTP i IMAP zanim dotrą one na komputer użytkownika, usuń zaznaczenie z pola **Skanuj ruch POP3, SMTP, NNTP i IMAP**. W tym przypadku wiadomości są skanowane przez rozszerzenie Ochrony poczty osadzone w programie pocztowym Microsoft Office Outlook po dotarciu na komputer użytkownika, jeśli zaznaczone jest pole **Włącz rozszerzenie Microsoft Outlook**.

Jeśli korzystasz z klienta poczty innego niż Microsoft Office Outlook, komponent Ochrona poczty nie skanuje wiadomości przesyłanych poprzez protokoły POP3, SMTP, NNTP i IMAP, jeśli pole **Skanuj ruch POP3, SMTP, NNTP i IMAP** nie jest zaznaczone.

- Jeśli chcesz umożliwić dostęp do ustawień Ochrony poczty z poziomu Microsoft Office Outlook i włączyć skanowanie wiadomości pocztowych przesyłanych poprzez protokoły POP3, SMTP, NNTP, IMAP i MAPI po ich odebraniu na komputerze przez wtyczkę wbudowaną w Microsoft Office Outlook, zaznacz pole **Włącz rozszerzenie Microsoft Outlook**.

Jeśli chcesz zablokować dostęp do ustawień Ochrony poczty z poziomu Microsoft Office Outlook i wyłączyć skanowanie wiadomości pocztowych przesyłanych poprzez protokoły POP3, SMTP, NNTP, IMAP i MAPI po ich odebraniu na komputerze przez wtyczkę wbudowaną w Microsoft Office Outlook, usuń zaznaczenie z pola **Włącz rozszerzenie Microsoft Outlook**.


Rozszerzenie Ochrony poczty jest integrowane z programem pocztowym Microsoft Office Outlook w trakcie instalacji Kaspersky Endpoint Security.

6. Zapisz swoje zmiany.

Skanowanie plików złożonych załączonych do wiadomości e-mail

Możesz włączyć lub wyłączyć skanowanie załączników w wiadomościach, ograniczyć maksymalny rozmiar skanowanych załączników, a także ograniczyć maksymalny czas skanowania załączników.

W celu skanowania plików złożonych załączonych do wiadomości e-mail:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. W sekcji **Skanuj pliki złożone** skonfiguruj ustawienia skanowania:
 - **Skanuj załączone pliki formatów pakietu Office**. Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty.
 - **Skanuj załączone archiwa**. Skanuje archiwa w następujących formatach: RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.

Jeżeli podczas skanowania Kaspersky Endpoint Security wykryje w tekście wiadomości hasło do archiwum, hasło to zostanie wykorzystane do przeskanowania zawartości archiwum w poszukiwaniu szkodliwych aplikacji. W tym przypadku hasło nie zostaje zapisane. Archiwum jest rozpakowywane podczas skanowania. Jeśli podczas rozpakowywania wystąpi błąd aplikacji, można ręcznie usunąć rozpakowane pliki, które są zapisywane w następującej ścieżce: %systemroot%\temp. Pliki mają prefiks PR.

- **Nie skanuj archiwów większych niż N MB**. Jeżeli pole jest zaznaczone, moduł Ochrona poczty wyklucza ze skanowania archiwa, załączone do wiadomości, których rozmiar przekracza określoną wartość. Jeżeli pole nie jest zaznaczone, moduł Ochrona poczty skanuje załączone archiwa o dowolnym rozmiarze.
- **Ogranicz czas sprawdzania archiwów do N s**. Jeżeli pole jest zaznaczone, czas skanowania archiwów załączonych do wiadomości e-mail jest ograniczony.


5. Zapisz swoje zmiany.

Filtrowanie załączników wiadomości e-mail

Funkcjonalność filtrowania załączników nie jest stosowana do wychodzących wiadomości e-mail.

Szkodliwe aplikacje mogą być rozpowszechniane w postaci załączników w wiadomościach e-mail. Możesz skonfigurować filtrowanie w oparciu o typ załączników wiadomości, aby automatycznie usuwano lub zmieniano nazwy plików określonych typów. Poprzez zmianę nazwy załącznika określonego typu, Kaspersky Endpoint Security może ochronić Twój komputer przed automatycznym wykonaniem szkodliwej aplikacji.

W celu skonfigurowania filtrowania załączników:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
3. Kliknij przycisk **Ustawienia zaawansowane**.
4. W sekcji **Filtr załączników** wykonaj jedną z następujących czynności:
 - **Wyłącz filtrowanie**. Jeśli ta opcja jest wybrana, Ochrona poczty nie filtruje plików załączonych do wiadomości e-mail.
 - **Zmień nazwy załączników określonych typów**. Jeśli wybierzesz tę opcję, Ochrona poczty zastąpi ostatni znak rozszerzenia wykryty w załączonych plikach określonych typów znakiem podkreślenia (na przykład: attachment.doc_). Dlatego, aby otworzyć plik, użytkownik musi zmienić jego nazwę.
 - **Usuń załączniki wybranych typów**. Jeśli ta opcja jest zaznaczona, Ochrona poczty usuwa załączone pliki określonych typów z wiadomości e-mail.
5. Jeśli w poprzednim kroku wybrałeś opcję **Zmień nazwy załączników określonych typów** lub opcję **Usuń załączniki wybranych typów**, zaznacz pola obok odpowiednich typów plików.
6. Zapisz swoje zmiany.

Eksportowanie i importowanie rozszerzeń dla filtrowania załączników

Możesz wyeksportować listę rozszerzeń filtra załączników do pliku XML. Możesz użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy rozszerzeń lub przeniesienia listy na inny serwer.

[Eksportowanie i importowanie listy rozszerzeń filtra załączników w Konsoli administracyjnej \(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
6. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
7. W otwartym oknie wybierz zakładkę **Filtr załączników**.
8. W celu wyeksportowania listy rozszerzeń:
 - a. Wybierz rozszerzenia, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę rozszerzeń, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security wyeksportuje całą listę rozszerzeń do pliku XML.
9. W celu zaimportowania listy rozszerzeń:
 - a. Kliknij odnośnik **Importuj**.
 - b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę rozszerzeń.
 - c. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę rozszerzeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
10. Zapisz swoje zmiany.

[Eksportowanie i importowanie listy rozszerzeń filtra załączników w Web Console i Cloud Console](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listę wykluczeń.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
5. W celu wyeksportowania listy rozszerzeń w sekcji **Filtr załączników**:
 - a. Wybierz rozszerzenia, które chcesz wyeksportować.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę rozszerzeń, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security wyeksportuje całą listę rozszerzeń do pliku XML.
6. W celu zaimportowania listy rozszerzeń w sekcji **Filtr załączników**:
 - a. Kliknij odnośnik **Importuj**.
 - b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę rozszerzeń.
 - c. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę rozszerzeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
7. Zapisz swoje zmiany.

Skanowanie poczty elektronicznej w programie Microsoft Office Outlook

Podczas instalacji Kaspersky Endpoint Security rozszerzenie Ochrony poczty jest osadzone w kliencie poczty Microsoft Office Outlook (zwany dalej także Outlook). Umożliwia ono szybkie przełączanie do ustawień Ochrony poczty z poziomu programu Outlook, a także określenie, kiedy wiadomość ma być skanowana w poszukiwaniu wirusów i innych zagrożeń. Rozszerzenie Ochrony poczty dla programu Outlook skanuje wiadomości wychodzące i przychodzące poprzez protokoły POP3, SMTP, NNTP, IMAP i MAPI. Kaspersky Endpoint Security obsługuje również współpracę z innymi klientami poczty e-mail (w tym Microsoft Outlook Express®, Poczta systemu Windows i Mozilla™ Thunderbird™).

Rozszerzenie Mail Threat Protection obsługuje działanie Outlook 2010, 2013, 2016, and 2019.

Podczas pracy z programem Mozilla Thunderbird moduł Ochrona poczty nie skanuje w poszukiwaniu wirusów i innych zagrożeń wiadomości przesyłanych poprzez protokół IMAP, jeśli filtry są wykorzystywane do przenoszenia wiadomości z folderu **Skrzynka odbiorcza**.

W programie Outlook wiadomości przychodzące są najpierw skanowane przez Ochronę poczty (jeżeli w interfejsie Kaspersky Endpoint Security zaznaczone jest pole [skanuj ruch POP3, SMTP, NNTP i IMAP](#)), a dopiero później przez rozszerzenie Ochrony poczty osadzone w programie Outlook. Jeżeli Ochrona poczty wykryje w wiadomości szkodliwy obiekt, wyświetli odpowiedni komunikat.

Ustawienia Ochrony poczty mogą zostać skonfigurowane bezpośrednio w programie Outlook, jeśli w interfejsie Kaspersky Endpoint Security zaznaczono pole [Rozszerzenie Microsoft Outlook zostało podłączone](#).

Wychodzące wiadomości są najpierw skanowane przez rozszerzenie Ochrony poczty osadzone w programie Outlook, a dopiero później przez Ochronę poczty.

Jeśli poczta jest skanowana przy użyciu rozszerzenia Ochrony poczty dla programu Outlook, zalecane jest korzystanie z trybu buforowanego programu Exchange. Więcej informacji dotyczących trybu buforowanego programu Exchange oraz zalecenia dotyczące korzystania z tego trybu można znaleźć w [Bazie wiedzy Microsoft](#).

W celu skonfigurowania trybu działania rozszerzenia modułu Ochrona poczty Outlook przy użyciu Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona poczty**.
6. W sekcji **Poziom ochrony** kliknij przycisk **Ustawienia**.
7. W sekcji **Łączność** kliknij **Ustawienia**.
8. W oknie **Ochrona poczty**:
 - Zaznacz pole **Skanuj podczas odbierania**, jeśli chcesz, żeby rozszerzenie Ochrony poczty dla programu Outlook skanowało wiadomości przychodzące w momencie pojawienia się w skrzynce odbiorczej.
 - Zaznacz pole **Skanuj podczas odczytu**, jeśli chcesz, żeby rozszerzenie Ochrony poczty dla programu Outlook skanowało wiadomości przychodzące w momencie otwarcia ich przez użytkownika.
 - Zaznacz pole **Skanuj podczas wysyłania**, jeśli chcesz, żeby rozszerzenie Ochrony poczty dla programu Outlook skanowało wiadomości wychodzące w momencie ich wysyłania.
9. Zapisz swoje zmiany.


Ochrona sieci

Moduł Ochrona sieci bada przychodzący ruch sieciowy pod kątem aktywności typowych dla ataków sieciowych. Jeśli Kaspersky Endpoint Security wykryje próbę ataku sieciowego na komputerze użytkownika, zablokuje połączenie sieciowe z komputerem atakującym. Opisy znanych typów ataków sieciowych oraz sposoby ich zwalczania znajdują się w bazach danych programu Kaspersky Endpoint Security. Lista ataków sieciowych, wykrywanych przez komponent Ochrona sieci, jest uaktualniana podczas [aktualizacji baz danych i modułów aplikacji](#).

Włączanie i wyłączanie modułu Ochrona sieci

Domyślnie moduł Ochrona sieci jest włączony i działa w trybie optymalnym. W razie konieczności możesz wyłączyć Ochronę sieci.


W celu włączenia lub wyłączenia Ochrony sieci:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona sieci**.
3. Użyj przełącznika **Ochrona sieci**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Ochrona sieci jest włączona, Kaspersky Endpoint Security skanuje przychodzący ruch sieciowy dla aktywności, która jest typowa dla ataków sieciowych. Jeśli Kaspersky Endpoint Security wykryje próbę ataku sieciowego na komputerze użytkownika, zablokuje połączenie sieciowe z komputerem atakującym.

Blokowanie atakującego komputera

W celu zablokowania atakującego komputera:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona sieci**.
3. Zaznacz pole **Dodaj atakujący komputer do listy zablokowanych komputerów na N min.**

Jeśli pole jest zaznaczone, Ochrona sieci dodaje atakujący komputer do listy zablokowanych. Oznacza to, że komponent Ochrona sieci zablokuje na określony czas połączenie sieciowe z atakującym komputerem po pierwszej próbie ataku sieciowego. Ta blokada automatycznie chroni komputer użytkownika przed przyszłymi atakami sieciowymi pochodzącymi z tego samego adresu.

W oknie [Narzędzia Monitor sieci](#) możesz przejrzeć listę blokowania.

Kaspersky Endpoint Security czyści listę blokowania, gdy aplikacja zostanie ponownie uruchomiona, a ustawienia Ochrony sieci zostaną zmienione.

4. Ustaw inny czas trwania blokowania dla atakującego komputera w polu po prawej stronie pola **Dodaj atakujący komputer do listy blokowanych komputerów na N min.**


5. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Kaspersky Endpoint Security wykryje próbę ataku sieciowego skierowanego na komputer użytkownika, zablokuje wszelkie połączenia z atakującym komputerem.

Konfigurowanie wykluczania adresów z blokowania

Kaspersky Endpoint Security może rozpoznać atak sieciowy i zablokować niezabezpieczone połączenie sieciowe, za pośrednictwem którego przesyłana jest duża liczba pakietów (na przykład: z kamer nadzorujących). Aby móc pracować z zaufanymi urządzeniami, możesz dodać adresy IP tych urządzeń do listy wykluczeń.

W celu skonfigurowania wykluczenia adresów z blokowania:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona sieci**.
3. Kliknij odnośnik **Zarządzaj wykluczeniami**.
4. W oknie kliknij przycisk **Dodaj**.
5. Wprowadź adres IP komputera, z którego ataki sieciowe nie będą blokowane.
6. Zapisz swoje zmiany.

W wyniku tego działania program Kaspersky Endpoint Security nie śledzi aktywności pochodzącej z urządzeń, które znajdują się na liście wykluczeń.

Eksportowanie i importowanie listy wykluczeń z blokowania

Możesz wyeksportować listę wykluczeń do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę adresów tego samego typu. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy wykluczeń lub przeniesienia listy na inny serwer.

[Eksportowanie i importowanie listy wykluczeń w Konsoli administracyjnej.\(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona sieci**.
6. W sekcji **Ustawienia Ochrony sieci** kliknij przycisk **Wykluczenia**.
7. W celu wyeksportowania listy reguł:
 - a. Wybierz wykluczenia, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
Jeśli nie wybrałeś żadnego wykluczenia, Kaspersky Endpoint Security wyeksportuje wszystkie wykluczenia.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML.
8. W celu zaimportowania listy wykluczeń:
 - a. Kliknij przycisk **Importuj**.
 - b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.
 - c. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
9. Zapisz swoje zmiany.

[Eksportowanie i importowanie listy wykluczeń w Web Console i Cloud Console](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listę wykluczeń.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona sieci**.
5. W sekcji **Ustawienia Ochrony sieci** kliknij odnośnik **Wykluczenia**.
Zostanie otwarta lista wykluczeń.
6. W celu wyeksportowania listy reguł:
 - a. Wybierz wykluczenia, które chcesz wyeksportować.
 - b. Kliknij przycisk **Eksportuj**.
 - c. Potwierdź chęć wyeksportowania tylko wybranych wykluczeń lub wyeksportuj całą listę wykluczeń.
 - d. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
 - e. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML.
7. W celu zaimportowania listy wykluczeń:
 - a. Kliknij przycisk **Importuj**.
 - b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.
 - c. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.

Konfigurowanie ochrony przed atakami sieciowymi według typu

Kaspersky Endpoint Security umożliwia zarządzanie ochroną przed następującymi typami ataków sieciowych:

- *Zalewanie sieci* jest atakiem na zasoby sieciowe (takie jak serwery internetowe). Ten atak obejmuje wysyłanie dużej liczby żądań w celu przeciążenia przepustowości zasobów sieciowych. W takiej sytuacji użytkownicy nie mogą uzyskać dostępu do zasobów sieciowych organizacji.
- Atak *Skanowanie portów* obejmuje skanowanie portów UDP, portów TCP, a także usługi sieciowe komputera. Ten atak umożliwia atakującemu zidentyfikowanie stopnia podatności komputera przed przeprowadzeniem bardziej niebezpiecznych rodzajów ataków sieciowych. Skanowanie portów umożliwia atakującemu także


zidentyfikowanie systemu operacyjnego na komputerze i wybranie odpowiednich ataków sieciowych dla tego systemu operacyjnego.

- *Atak przez fałszowanie adresu MAC* obejmuje zmianę adresu MAC urządzenia sieciowego (karty sieciowej). W rezultacie osoba atakująca może przekierować dane wysłane do urządzenia na inne urządzenie i uzyskać dostęp do tych danych. Kaspersky Endpoint Security umożliwia blokowanie ataków przez fałszowanie adresu MAC i otrzymywanie powiadomień o atakach.

Możesz wyłączyć wykrywanie tych rodzajów ataków w przypadku, gdy niektóre z Twoich dozwolonych aplikacji wykonują działania typowe dla tych rodzajów ataków. Pomoże to w uniknięciu fałszywych alarmów.

Domyślnie, Kaspersky Endpoint Security nie monitoruje ataków typu zalewanie sieci, skanowanie portów, a także ataku przez fałszowanie adresu MAC.

W celu skonfigurowania ochrony przed atakami sieciowymi według typu:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona sieci**.
3. Użyj przełącznika **Traktuj skanowanie portów i zalewanie sieci jako ataki**, aby włączyć lub wyłączyć wykrywanie tych ataków.
4. Użyj przełącznika **Ochrona przed fałszowaniem adresu MAC**.
5. W sekcji **Po wykryciu ataku fałszującego adres MAC** wybierz jedną z następujących opcji:
 - **Tylko powiadom.**
 - **Powiadom i zablokuj.**
6. Zapisz swoje zmiany.

Zapora sieciowa

Zapora sieciowa blokuje nieautoryzowane połączenia z komputerem podczas pracy w internecie lub sieci lokalnej. Zapora sieciowa kontroluje również aktywność sieciową aplikacji na komputerze. Pozwala to chronić korporacyjną sieć LAN przed kradzieżą tożsamości i innymi atakami. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i predefiniowanych *reguł sieciowych*.

Agent sieciowy jest używany do interakcji z Kaspersky Security Center. Zapora sieciowa automatycznie tworzy reguły sieciowe wymagane do działania aplikacji i Agenta sieciowego. W wyniku działania Zapora sieciowa otwiera kilka portów na komputerze. Które porty są otwarte w zależności od roli komputera (na przykład, punkt dystrybucji). Więcej informacji o portach, które zostaną otwarte na komputerze, można znaleźć w [pomocy dla Kaspersky Security Center](#).

Reguły sieciowe

Możesz skonfigurować reguły sieciowe na następujących poziomach:

- *Reguły pakietów sieciowych.* Reguły pakietów sieciowych nakładają ograniczenia na pakiety sieciowe, niezależnie od aplikacji. Takie reguły ograniczają ruch sieciowy wychodzący i przychodzący przez określone porty wybranego protokołu. Kaspersky Endpoint Security wstępnie zdefiniował reguły pakietów sieciowych z uprawnieniami zalecanymi przez ekspertów z Kaspersky.
- *Reguły sieciowe dla aplikacji.* Reguły sieciowe dla aplikacji nakładają ograniczenia na aktywność sieciową określonej aplikacji. W tym przypadku brane są pod uwagę cechy charakterystyczne pakietu sieciowego, a także aplikacja, dla której jest on przeznaczony lub która zainicjowała jego przesyłanie.

Kontrolowany dostęp aplikacji do zasobów systemu operacyjnego, procesów i danych osobowych jest zapewniany przez [komponent Ochrona przed włamaniami](#) przy użyciu *uprawnień aplikacji*.

Podczas pierwszego uruchomienia aplikacji Zapora sieciowa wykonuje następujące działania:

1. Sprawdza bezpieczeństwo aplikacji przy użyciu pobranych antywirusowych baz danych.
2. Sprawdza bezpieczeństwo aplikacji w Kaspersky Security Network.
Zalecane jest [uczestniczenie w Kaspersky Security Network](#), aby zapewnić bardziej efektywne działanie Zapory sieciowej.
3. Umieszcza aplikację w jednej z *grup zaufania*: Zaufane, Niski poziom ograniczeń, Wysoki poziom ograniczeń, Niezaufane.

[Grupa zaufania określa uprawnienia](#), do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.

Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania dla składników Zapora sieciowa i Ochrona przed włamaniami. Nie można zmienić grupy zaufania tylko dla Zapory sieciowej lub Ochrony przed włamaniami.

Jeśli odmówiłeś uczestnictwa w KSN lub nie ma sieci, Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od [ustawień modułu Ochrona przed włamaniami](#). Po otrzymaniu reputacji aplikacji od KSN, grupę zaufania można zmienić automatycznie.

4. Blokuje aktywność sieciową aplikacji w zależności od grupy zaufania. Na przykład, aplikacje z grupy Wysoki poziom ograniczeń nie mogą korzystać z żadnych połączeń sieciowych.

Przy następnym uruchomieniu aplikacji, Kaspersky Endpoint Security sprawdzi integralność aplikacji. Jeżeli aplikacja nie została zmieniona, moduł użyje dla niej bieżących reguł sieciowych. Jeżeli aplikacja została zmodyfikowana, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

Priorytety reguł sieciowych

Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli aktywność sieci zostanie dodana do kilku reguł, Zapora sieciowa reguluje aktywność sieciową zgodnie z regułą o najwyższym priorytecie.

Reguły pakietów sieciowych mają wyższy priorytet niż reguły sieciowe dla aplikacji. Jeżeli do tego samego typu aktywności sieciowej są zastosowane reguły pakietów sieciowych i reguły sieciowe dla aplikacji, będzie ona przetwarzana zgodnie z regułami pakietów sieciowych.

Reguły sieciowe dla aplikacji działają w następujący sposób: reguła sieciowa dla aplikacji obejmuje reguły dostępu oparte na stanie sieci: *publiczna*, *lokalna* lub *zaufana*. Na przykład, aplikacje z grupy zaufania Wysoki poziom ograniczeń domyślnie nie zezwalają na żadną aktywność sieciową w sieciach o wszystkich stanach. Jeśli dla pojedynczej aplikacji (aplikacji nadrzędnej) zostanie określona reguła sieciowa, procesy potomne innych aplikacji będą działać zgodnie z regułą sieciową aplikacji nadrzędnej. Jeśli nie istnieje reguła sieciowa dla aplikacji, procesy potomne będą działały zgodnie z regułą dostępu do sieci grupy zaufania aplikacji.

Na przykład, zabroniona jest jakakolwiek aktywność sieciowa w sieciach o wszystkich stanach dla wszystkich aplikacji, za wyjątkiem przeglądarki X. Jeśli rozpoczniesz instalację przeglądarki Y (proces potomny) z przeglądarki X (aplikacja nadrzędna), wówczas instalator przeglądarki Y uzyska dostęp do sieci i pobierze niezbędne pliki. Po instalacji przeglądarka Y będzie odmawiała jakichkolwiek połączeń sieciowych zgodnie z ustawieniami Zapory sieciowej. Aby zabronić aktywności sieciowej instalatora przeglądarki Y jako procesu potomnego, należy dodać regułę sieciową dla instalatora przeglądarki Y.

Stany połączenia sieciowego

Zapora sieciowa pozwala kontrolować aktywność sieciową w zależności od stanu połączenia sieciowego. Kaspersky Endpoint Security otrzymuje stan połączenia sieciowego z systemu operacyjnego komputera. Stan połączenia sieciowego w systemie operacyjnym jest ustawiany przez użytkownika podczas konfigurowania połączenia. Możesz [zmienić stan połączenia sieciowego w ustawieniach Kaspersky Endpoint Security](#). Zapora sieciowa będzie monitorować aktywność sieci w zależności od stanu sieci w ustawieniach Kaspersky Endpoint Security, a nie w systemie operacyjnym.

Połączenie sieciowe może mieć jeden z następujących typów stanu:

- **Sieć publiczna.** Sieć nie jest chroniona przez aplikacje antywirusowe, zapory sieciowe ani filtry (takie jak Wi-Fi w kawiarni). Podczas korzystania z komputera podłączonego do tego typu sieci Zapora sieciowa blokuje dostęp do plików i drukarek tego komputera. Użytkownicy z zewnątrz nie będą mogli również uzyskać dostępu do danych poprzez folder współdzielony oraz zdalnego dostępu do pulpitu tego komputera. Zapora sieciowa filtruje aktywność sieciową każdej aplikacji zgodnie z utworzoną dla niej regułą sieciową.


Domyślnie do internetu przypisywany jest stan *Sieć publiczna*. Nie możesz zmienić stanu przypisanego do internetu.

- **Sieć lokalna.** Sieć dla użytkowników z ograniczonym dostępem do plików i drukarek na tym komputerze (na przykład dla firmowej sieci LAN lub sieci domowej).
- **Sieć zaufana.** Bezpieczna sieć, w której komputer nie jest wystawiony na ataki lub nieautoryzowane próby dostępu do danych. Zapora sieciowa zezwala na dowolną aktywność sieciową w obrębie sieci o tym stanie.

Włączanie i wyłączanie modułu Zapora sieciowa

Domyślnie moduł Zapora sieciowa jest włączony i działa w trybie optymalnym.


W celu włączenia i wyłączenia modułu Zapora sieciowa:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Użyj przełącznika **Zapora sieciowa**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

Zmianie stanu połączenia sieciowego

Domyślnie do internetu przypisywany jest stan *Sieć publiczna*. Nie możesz zmienić stanu przypisanego do internetu.

W celu zmiany stanu połączenia sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij przycisk **Dostępne sieci**.
4. Wybierz połączenie sieciowe, którego stan chcesz zmienić.
5. W kolumnie **Typ sieci** wybierz stan połączenia sieciowego:
 - **Sieć publiczna**. Sieć nie jest chroniona przez aplikacje antywirusowe, zapory sieciowe ani filtry (takie jak Wi-Fi w kawiarni). Podczas korzystania z komputera podłączonego do tego typu sieci Zapora sieciowa blokuje dostęp do plików i drukarek tego komputera. Użytkownicy z zewnątrz nie będą mogli również uzyskać dostępu do danych poprzez folder współdzielony oraz zdalnego dostępu do pulpitu tego komputera. Zapora sieciowa filtruje aktywność sieciową każdej aplikacji zgodnie z utworzoną dla niej regułą sieciową.
 - **Sieć lokalna**. Sieć dla użytkowników z ograniczonym dostępem do plików i drukarek na tym komputerze (na przykład dla firmowej sieci LAN lub sieci domowej).
 - **Sieć zaufana**. Bezpieczna sieć, w której komputer nie jest wystawiony na ataki lub nieautoryzowane próby dostępu do danych. Zapora sieciowa zezwala na dowolną aktywność sieciową w obrębie sieci o tym stanie.
6. Zapisz swoje zmiany.

Zarządzanie regułami dla pakietów sieciowych

Podczas zarządzania regułami dla pakietów sieciowych możesz wykonać następujące czynności:

- **Utworzyć nową regułę dla pakietu sieciowego.**
Możesz utworzyć nową regułę dla pakietu sieciowego, tworząc zestaw warunków i akcji stosowany do pakietów sieciowych i strumieni danych.
- **Włączyć lub wyłączyć regułę dla pakietu sieciowego.**
Wszystkie reguły pakietów sieciowych utworzone przez Zaporę sieciową domyślnie posiadają stan *Włączona*. Jeżeli reguła dla pakietu sieciowego jest włączona, Zapora sieciowa stosuje tę regułę.
Możesz wyłączyć dowolną regułę dla pakietu sieciowego, która została wybrana z listy reguł dla pakietów sieciowych. Jeżeli reguła dla pakietu sieciowego jest wyłączona, Zapora sieciowa tymczasowo nie stosuje tej reguły.

Nowa niestandardowa reguła dla pakietu sieciowego jest dodawana do listy reguł dla pakietów sieciowych z domyślnym stanem *Włączona*.

- Zmodyfikować ustawienia już istniejącej reguły dla pakietu sieciowego.
Po utworzeniu nowej reguły dla pakietu sieciowego, można zawsze powrócić do edycji jej ustawień i w razie potrzeby zmodyfikować je.
- Zmienić akcję Zapory sieciowej dla reguły dla pakietu sieciowego.
Na liście reguł dla pakietów sieciowych możesz zmodyfikować akcję podejmowaną przez Zaporę sieciową po wykryciu aktywności sieciowej odpowiadającej określonej regule dla pakietu sieciowego.
- Zmienić priorytet reguły dla pakietu sieciowego.
Możesz zwiększyć lub zmniejszyć priorytet wybranej reguły dla pakietu sieciowego.
- Usunąć regułę dla pakietu sieciowego.
Możesz usunąć regułę dla pakietu sieciowego, aby Zapora sieciowa przestała stosować ją po wykryciu aktywności sieciowej, a także aby reguła ta nie była wyświetlana na liście reguł dla pakietów sieciowych ze stanem *Wyłączona*.

Tworzenie reguły dla pakietu sieciowego.

Regułę dla pakietu sieciowego można utworzyć na następujące sposoby:


- Użyj [narzędzia Monitor sieci](#).
Monitor sieci to narzędzie służące do wyświetlania informacji o aktywności sieciowej komputera użytkownika w czasie rzeczywistym. Jest to wygodne, ponieważ nie potrzebujesz konfigurować wszystkich ustawień reguły. Niektóre ustawienia Zapory sieciowej zostaną automatycznie uzupełnione z danych Monitora sieci. Monitor sieci jest dostępny tylko w interfejsie aplikacji.
- Skonfiguruj ustawienia Zapory sieciowej.
To umożliwi dostosowanie ustawień Zapory sieciowej. Możesz utworzyć reguły dla dowolnej aktywności sieciowej nawet wtedy, gdy aktualnie nie ma aktywności sieciowej.

Podczas tworzenia reguł dla pakietów sieciowych należy pamiętać, że posiadają one wyższy priorytet niż reguły sieciowe dla aplikacji.


[Jak używać narzędzia Monitor sieci do utworzenia reguły dla pakietu sieciowego w interfejsie aplikacji?](#) 

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Monitor sieci**.
2. Wybierz zakładkę **Aktywność sieciowa**.
Zakładka **Aktywność sieciowa** wyświetla wszystkie aktualnie aktywne połączenia sieciowe komputera. Wyświetlane są połączenia przychodzące i wychodzące.
3. Z menu kontekstowego połączenia sieciowego wybierz **Utwórz regułę dla pakietu sieciowego**.
Spowoduje to otwarcie właściwości reguły sieciowej.
4. Ustaw stan **Aktywny** dla reguły dla pakietów.
5. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
6. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).
Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Szablon reguły sieciowej**. Szablony reguły opisują najczęściej używane połączenia sieciowe.
Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
7. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w [raporcie](#), zaznacz pole **Zapisuj zdarzenia**.
8. Kliknij przycisk **Zapisz**.
Nowa reguła sieciowa zostanie dodana do listy.
9. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
10. Zapisz swoje zmiany.

[Jak używać ustawień Zapory sieciowej do utworzenia reguły dla pakietu sieciowego w interfejsie aplikacji?](#) 

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij przycisk **Reguły dla pakietów**.
Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
4. Kliknij przycisk **Dodaj**.
Spowoduje to otwarcie właściwości reguły sieciowej.
5. Ustaw stan **Aktywny** dla reguły dla pakietów.
6. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
7. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).
Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Szablon reguły sieciowej**. Szablony reguły opisują najczęściej używane połączenia sieciowe.
Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
8. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w [raporcie](#), zaznacz pole **Zapisuj zdarzenia**.
9. Kliknij przycisk **Zapisz**.
Nowa reguła sieciowa zostanie dodana do listy.
10. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
11. Zapisz swoje zmiany.

[Jak utworzyć regułę dla pakietu sieciowego w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
6. W sekcji **Ustawienia Zapory sieciowej** kliknij przycisk **Ustawienia**.
To spowoduje otwarcie listy reguł dla pakietów sieciowych oraz listy reguł sieciowych dla aplikacji.
7. Wybierz zakładkę **Reguły pakietów sieciowych**.
Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
8. Kliknij przycisk **Dodaj**.
Spowoduje to otwarcie właściwości reguły dla pakietów.
9. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
10. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).
Możesz wybrać predefiniowany szablon reguły, klikając przycisk . Szablony reguły opisują najczęściej używane połączenia sieciowe.
Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
11. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w [raporcie](#), zaznacz pole **Zapisuj zdarzenia**.
12. Kliknij przycisk **Zapisz**.
Nowa reguła sieciowa zostanie dodana do listy.
13. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
14. Zapisz swoje zmiany.

Zapora sieciowa będzie kontrolowała pakiety sieciowe zgodnie z regułą. Możesz wyłączyć regułę dla pakietów w Zaporze sieciowej bez usuwania jej z listy. W tym celu odznacz pole obok obiektu.

[Jak utworzyć regułę pakietów sieciowych w Web Console i Cloud Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
5. W sekcji **Ustawienia Zapory sieciowej** kliknij odnośnik **Reguły pakietów sieciowych**.
Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
6. Kliknij przycisk **Dodaj**.
Spowoduje to otwarcie właściwości reguły dla pakietów.
7. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
8. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).
Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Wybierz szablon**. Szablony reguły opisują najczęściej używane połączenia sieciowe.
Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
9. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w [raporcie](#), zaznacz pole **Zapisuj zdarzenia**.
10. Kliknij przycisk **Zapisz**.
Nowa reguła sieciowa zostanie dodana do listy.
11. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
12. Zapisz swoje zmiany.

Zapora sieciowa będzie kontrolowała pakiety sieciowe zgodnie z regułą. Możesz wyłączyć regułę dla pakietów w Zaporze sieciowej bez usuwania jej z listy. Użyj przełącznika w kolumnie **Stan**, aby wyłączyć lub wyłączyć regułę dla pakietów.


Ustawienia reguły pakietów sieciowych

Parametr	Opis
Akcja	<p>Zezwól.</p> <p>Blokuj.</p> <p>Zgodnie z regułami aplikacji. Jeśli ta opcja jest zaznaczona, Zapora sieciowa stosuje reguły sieciowe dla aplikacji do połączenia sieciowego.</p>
Protokół	<p>Kontroluj aktywność sieciową poprzez wybrany protokół: TCP, UDP, ICMP, ICMPv6, IGMP i GRE.</p> <p>Jeśli wybrałeś protokół ICMP lub ICMPv6, możesz zdefiniować typ i kod pakietu ICMP.</p> <p>Jeżeli jako typ protokołu wybrałeś TCP lub UDP, możesz określić porty komputera lokalnego oraz komputera zdalnego (rozdzielając je przecinkami), między którymi połączenie będzie monitorowane.</p>
Kierunek	<p>Przychodzący (pakiet). Zapora sieciowa stosuje regułę sieciową do wszystkich przychodzących pakietów sieciowych.</p>

	<p>Przychodzący. Zapora sieciowa stosuje regułę sieciową do wszystkich pakietów sieciowych wysłanych za pośrednictwem połączenia zainicjowanego przez zdalny komputer.</p> <p>Przychodzący / Wychodzący. Zapora sieciowa stosuje regułę sieciową do wychodzących i przychodzących pakietów sieciowych bez względu na to, czy połączenie sieciowe zostało zainicjowane przez komputer użytkownika, czy zdalny komputer.</p> <p>Wychodzący (pakiet). Zapora sieciowa stosuje regułę sieciową do wszystkich wychodzących pakietów sieciowych.</p> <p>Wychodzący. Zapora sieciowa stosuje regułę sieciową do wszystkich pakietów sieciowych wysłanych za pośrednictwem połączenia zainicjowanego przez komputer użytkownika.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Protokół TCP nawiązuje połączenie. Dla TCP użyj kierunku: Przychodzący, Wychodzący i Przychodzący/Wychodzący. Wszystkie pozostałe protokoły nie nawiązują połączeń, ale wysyłają pakiety. Dla wszystkich pozostałych protokołów użyj kierunków: Przychodzący (pakiet), Wychodzący (pakiet) lub Przychodzący/Wychodzący.</p> </div>
Karty sieciowe	Karty sieciowe, które mogą wysłać i/lub odbierać pakiety sieciowe. Podczas określania ustawień kart sieciowych możliwe jest rozróżnienie pomiędzy pakietami sieciowymi wysłanymi lub odbieranymi przez karty sieciowe z takimi samymi adresami IP.
Czas wygaśnięcia (TTL)	Ogranicz kontrolę pakietów sieciowych w oparciu o ich czas wygaśnięcia (TTL).
Adresy zdalne	Adresy sieciowe zdalnych komputerów, które mogą wysłać i/lub odbierać pakiety sieciowe. Zapora sieciowa stosuje regułę sieciową do określonego zakresu zdalnych adresów sieciowych. Możesz włączyć wszystkie adresy IP do reguły sieciowej, utworzyć oddzielną listę adresów IP, określić zakres adresów IP lub wybrać podsieć (Sieci zaufane, Sieci lokalne, Sieci publiczne). Możesz także określić nazwę DNS komputera zamiast jego adresu IP. Powinieneś używać nazw DNS tylko dla komputerów LAN lub wewnętrznych usług. Interakcja z usługami chmury (takimi jak Microsoft Azure) i innymi zasobami internetowymi powinna być zarządzana przez komponent Kontrola sieci.
Adresy lokalne	Adresy sieciowe komputerów, które mogą wysłać i odbierać pakiety sieciowe. Zapora sieciowa stosuje regułę sieciową do określonego zakresu lokalnych adresów sieciowych. Możesz włączyć wszystkie adresy IP do reguły sieciowej, utworzyć oddzielną listę adresów IP lub określić zakres adresów IP. Możesz także określić nazwę DNS komputera zamiast jego adresu IP. Powinieneś używać nazw DNS tylko dla komputerów LAN lub wewnętrznych usług. Interakcja z usługami chmury (takimi jak Microsoft Azure) i innymi zasobami internetowymi powinna być zarządzana przez komponent Kontrola sieci.
	<div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Zdarza się, że dla aplikacji nie można uzyskać adresu lokalnego. W takim przypadku ten parametr jest ignorowany.</p> </div>

Włączanie i wyłączanie reguły dla pakietu sieciowego

W celu włączenia lub wyłączenia reguły dla pakietu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.

3. Kliknij przycisk **Reguły dla pakietów**.

Spowoduje to otwarcie listy domyślnych reguł dla pakietów sieciowych, ustawionych przez Zaporę sieciową.

4. Na liście wybierz żądaną regułę dla pakietu sieciowego.

5. Użyj przełącznika w kolumnie **Stan**, aby włączyć lub wyłączyć regułę.

6. Zapisz swoje zmiany.

Zmianie akcji Zapory sieciowej dla reguły dla pakietu sieciowego

W celu zmiany akcji Zapory sieciowej stosowanej do reguły dla pakietu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.

3. Kliknij przycisk **Reguły dla pakietów**.

Spowoduje to otwarcie listy domyślnych reguł dla pakietów sieciowych, ustawionych przez Zaporę sieciową.

4. Wybierz ją na liście reguł dla pakietów sieciowych i kliknij przycisk **Edytuj**.

5. Z listy rozwijalnej **Akcja** wybierz akcję, jaka zostanie wykonana przez Zaporę sieciową po wykryciu tego rodzaju aktywności sieciowej:

- **Zezwól.**
- **Blokuj.**
- **Zgodnie z regułami aplikacji.**

6. Zapisz swoje zmiany.

Zmianie priorytetu reguły dla pakietu sieciowego

Priorytet reguły dla pakietu sieciowego zależy od jej pozycji na liście reguł dla pakietów sieciowych. Reguła znajdująca się na najwyższej pozycji na liście reguł dla pakietów sieciowych ma najwyższy priorytet.

Każda ręcznie utworzona reguła dla pakietu sieciowego jest umieszczana na końcu listy i posiada najniższy priorytet.

Zapora sieciowa wykonuje reguły w kolejności, w jakiej występują na liście reguł dla pakietów sieciowych (od góry do dołu). Zgodnie z każdą przetworzoną regułą dla pakietu sieciowego, która odpowiada określonemu połączeniu sieciowemu, Zapora sieciowa zezwala na lub blokuje dostęp sieciowy do adresu i portu określonego w ustawieniach tego połączenia sieciowego.

W celu zmiany priorytetu reguły dla pakietu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij przycisk **Reguły dla pakietów**.
Spowoduje to otwarcie listy domyślnych reguł dla pakietów sieciowych, ustawionych przez Zaporę sieciową.
4. Z listy wybierz regułę dla pakietu sieciowego, której priorytet chcesz zmienić.
5. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
6. Zapisz swoje zmiany.

Eksportowanie i importowanie reguł dla pakietów sieciowych

Możesz wyeksportować listę reguł dla pakietów sieciowych do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę reguł tego samego typu. Możesz użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy reguł dla pakietów sieciowych lub przeniesienia listy na inny serwer.

[Eksportowanie i importowanie listy reguł dla pakietów sieciowych w Konsoli administracyjnej \(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
6. W celu wyeksportowania listy reguł dla pakietów sieciowych:
 - a. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.
7. W celu zaimportowania listy reguł dla pakietów sieciowych:
 - a. Kliknij odnośnik **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
 - b. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.

[Eksportowanie i importowanie listy reguł dla pakietów sieciowych w Web Console i Cloud Console](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listę reguł.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
5. Kliknij odnośnik **Reguły pakietów sieciowych**.
6. W celu wyeksportowania listy reguł dla pakietów sieciowych:
 - a. Wybierz reguły, które chcesz zmienić.
 - b. Kliknij przycisk **Eksportuj**.
 - c. Potwierdź chęć wyeksportowania tylko wybranych reguł lub wyeksportuj całą listę.
 - d. Kliknij przycisk **Eksportuj**.
Kaspersky Endpoint Security eksportuje listę reguł do pliku XML w domyślnym folderze do pobrania.
7. W celu zaimportowania listy reguł dla pakietów sieciowych:
 - a. Kliknij odnośnik **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
 - b. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.

Zarządzanie regułami sieciowymi dla aplikacji

Domyślnie Kaspersky Endpoint Security grupuje wszystkie aplikacje zainstalowane na komputerze według nazwy producenta oprogramowania, którego aktywność sieciową lub plikową monitoruje. Grupy aplikacji są dzielone na [grupy zaufania](#). Wszystkie aplikacje i grupy aplikacji dziedziczą właściwości od grupy nadrzędnej: reguły kontroli aplikacji, reguły sieciowe dla aplikacji i ich priorytet wykonania.

Podobnie, jak w przypadku komponentu [Ochrona przed włamaniami](#), domyślnie moduł Zapora sieciowa stosuje reguły sieciowe do grupy aplikacji podczas filtrowania aktywności sieciowej wszystkich aplikacji w tej grupie. Reguły sieciowe dla grup aplikacji definiują dla aplikacji w obrębie grupy uprawnienia dostępu do różnych połączeń sieciowych.

Domyślnie Zapora sieciowa tworzy zestaw reguł sieciowych dla każdej grupy aplikacji wykrytej na komputerze przez Kaspersky Endpoint Security. Możesz zmienić akcję Zapory sieciowej stosowaną do domyślnie utworzonych reguł sieciowych dla grupy aplikacji. Nie można modyfikować, usuwać, wyłączać oraz zmieniać priorytetu domyślnie utworzonych reguł sieciowych dla grupy aplikacji.

Możesz także utworzyć regułę sieciową dla pojedynczej aplikacji. Taka reguła będzie miała wyższy priorytet niż reguła sieciowa grupy, do której należy aplikacja.

Tworzenie reguły sieciowej dla aplikacji

Domyślnie aktywność aplikacji jest kontrolowana przez reguły sieciowe, które są definiowane dla [grupy zaufania](#), do której Kaspersky Endpoint Security przypisał aplikację przy jej pierwszym uruchomieniu. Jeżeli jest to konieczne, możesz utworzyć reguły sieciowe dla całej grupy zaufania, dla pojedynczej aplikacji lub dla grupy aplikacji znajdujących się w grupie zaufania.

Ręcznie zdefiniowane reguły sieciowe posiadają wyższy priorytet niż reguły sieciowe, które zostały określone dla grupy zaufania. Innymi słowy, jeśli ręcznie zdefiniowane reguły dla aplikacji różnią się od reguł dla aplikacji określonych dla grupy zaufania, Zapora sieciowa kontroluje aktywność aplikacji zgodnie z ręcznie zdefiniowanymi regułami dla aplikacji.

Domyślnie, Zapora sieciowa tworzy następujące reguły sieciowe dla każdej aplikacji:

- Dowolna aktywność sieciowa w sieciach Zaufanych.
- Dowolna aktywność sieciowa w sieciach Lokalnych.
- Dowolna aktywność sieciowa w sieciach Publicznych.

Kaspersky Endpoint Security kontroluje aktywność sieciową aplikacji zgodnie z predefiniowanymi regułami sieciowymi w następujący sposób:

- Zaufane i Niski poziom ograniczeń: wszelka aktywność sieciowa jest dozwolona.
- Wysoki poziom ograniczeń i Niezaufane: wszelka aktywność sieciowa jest zablokowana.

Predefiniowane reguły aplikacji nie mogą być edytowane lub usuwane.

Możesz utworzyć regułę sieciową dla aplikacji w następujące sposoby:

- Użyj [narzędzia Monitor sieci](#).

Monitor sieci to narzędzie służące do wyświetlania informacji o aktywności sieciowej komputera użytkownika w czasie rzeczywistym. Jest to wygodne, ponieważ nie potrzebujesz konfigurować wszystkich ustawień reguły. Niektóre ustawienia Zapory sieciowej zostaną automatycznie uzupełnione z danych Monitora sieci. Monitor sieci jest dostępny tylko w interfejsie aplikacji.

- Skonfiguruj ustawienia Zapory sieciowej.


To umożliwi dostosowanie ustawień Zapory sieciowej. Możesz utworzyć reguły dla dowolnej aktywności sieciowej nawet wtedy, gdy aktualnie nie ma aktywności sieciowej.

Podczas tworzenia reguł sieciowych dla aplikacji pamiętaj, że reguły pakietów sieciowych posiadają priorytet wyższy niż reguły sieciowe dla aplikacji.


Jak używać narzędzia Monitor sieci do utworzenia reguły sieciowej dla aplikacji w interfejsie aplikacji?

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Monitor sieci**.
2. Wybierz zakładkę **Aktywność sieciowa** lub **Otwarte porty**.
Zakładka **Aktywność sieciowa** wyświetla wszystkie aktualnie aktywne połączenia sieciowe komputera. Wyświetlane są połączenia przychodzące i wychodzące.
Na zakładce **Otwarte porty** wyświetlane są wszystkie otwarte porty sieciowe komputera.
3. Z menu kontekstowego połączenia sieciowego wybierz **Utwórz regułę dla aplikacji**.
Zostanie otwarte okno właściwości i reguł aplikacji.
4. Zaznacz zakładkę **Reguły sieciowe**.
Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
5. Kliknij przycisk **Dodaj**.
Spowoduje to otwarcie właściwości reguły sieciowej.
6. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
7. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).
Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Szablon reguły sieciowej**. Szablony reguły opisują najczęściej używane połączenia sieciowe.
Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
8. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w [raporcie](#), zaznacz pole **Zapisuj zdarzenia**.
9. Kliknij przycisk **Zapisz**.
Nowa reguła sieciowa zostanie dodana do listy.
10. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
11. Zapisz swoje zmiany.

Jak używać ustawień Zapory sieciowej do utworzenia reguły sieciowej dla aplikacji w interfejsie aplikacji?

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij przycisk **Reguły aplikacji**.
Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
4. Na liście aplikacji wybierz aplikację lub grupę aplikacji, dla której chcesz utworzyć regułę sieciową.
5. Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Szczegóły i reguły**.
Zostanie otwarte okno właściwości i reguł aplikacji.
6. Zaznacz zakładkę **Reguły sieciowe**.
7. Kliknij przycisk **Dodaj**.
Spowoduje to otwarcie właściwości reguły sieciowej.
8. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
9. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).
Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Szablon reguły sieciowej**. Szablony reguły opisują najczęściej używane połączenia sieciowe.
Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
10. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w [raporcie](#), zaznacz pole **Zapisuj zdarzenia**.
11. Kliknij przycisk **Zapisz**.
Nowa reguła sieciowa zostanie dodana do listy.
12. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.
13. Zapisz swoje zmiany.

[Jak utworzyć regułę sieciową dla aplikacji w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
6. W sekcji **Ustawienia Zapory sieciowej** kliknij przycisk **Ustawienia**.
To spowoduje otwarcie listy reguł dla pakietów sieciowych oraz listy reguł sieciowych dla aplikacji.
7. Wybierz zakładkę **Reguły sieciowe dla aplikacji**.
8. Kliknij przycisk **Dodaj**.
9. W otwartym oknie wprowadź kryteria wyszukiwania aplikacji, dla których chcesz utworzyć regułę sieciową.
Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki * i ?.
10. Kliknij przycisk **Odśwież**.
Kaspersky Endpoint Security wyszuka aplikację na skonsolidowanej liście aplikacji zainstalowanych na zarządzanych komputerach. Kaspersky Endpoint Security wyświetli listę aplikacji spełniających Twoje kryteria wyszukiwania.
11. Wybierz żadaną aplikację.
12. Z listy rozwijalnej **Dodaj wybraną aplikację do grupy zaufania**<grupa zaufania> wybierz **Grupy domyślne** i kliknij **OK**.
Aplikacja zostanie dodana do domyślnej grupy.
13. Wybierz odpowiednią aplikację, a następnie wybierz **Uprawnienia aplikacji** z menu kontekstowego aplikacji.
Zostanie otwarte okno właściwości i reguł aplikacji.
14. Zaznacz zakładkę **Reguły sieciowe**.
Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
15. Kliknij przycisk **Dodaj**.
Spowoduje to otwarcie właściwości reguły sieciowej.
16. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
17. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).
Możesz wybrać predefiniowany szablon reguły, klikając przycisk . Szablony reguły opisują najczęściej używane połączenia sieciowe.
Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
18. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w [raporcie](#), zaznacz pole **Zapisuj zdarzenia**.
19. Kliknij przycisk **Zapisz**.

Nowa reguła sieciowa zostanie dodana do listy.

20. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.

21. Zapisz swoje zmiany.

[Jak utworzyć regułę sieciową dla aplikacji w Web Console i Cloud Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
5. W sekcji **Ustawienia Zapory sieciowej** kliknij odnośnik **Reguły sieciowe dla aplikacji**.
To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
6. Wybierz zakładkę **Uprawnienia aplikacji**.
W lewej części okna zobaczysz listę grup zaufania, a w prawej części okna zobaczysz i ich właściwości.
7. Kliknij przycisk **Dodaj**.
To spowoduje uruchomienie Kreatora dodawania aplikacji do grupy zaufania.
8. Wybierz odpowiednią grupę zaufania dla aplikacji.
9. Wybierz typ **Aplikacja**. Kliknij przycisk **Dalej**.
Jeśli chcesz utworzyć regułę sieciową dla kilku aplikacji, wybierz typ **Grupa** i określ nazwę grupy aplikacji.
10. Na otwartej liście aplikacji wybierz aplikacje, dla których chcesz utworzyć regułę sieciową.
Użyj filtra. Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki * i ?.
11. Zakończ działanie kreatora, klikając **OK**.
Aplikacja zostanie dodana do grupy zaufania.
12. W lewej części okna wybierz odpowiednią aplikację.
13. W prawej części okna, z listy rozwijalnej wybierz **Reguły sieciowe**.
Spowoduje to otwarcie listy domyślnych reguł sieciowych, ustawionych przez Zaporę sieciową.
14. Kliknij przycisk **Dodaj**.
Spowoduje to otwarcie właściwości reguły aplikacji.
15. W polu **Nazwa** wprowadź ręcznie nazwę usługi sieciowej.
16. Skonfiguruj ustawienia reguły sieciowej (patrz tabela poniżej).
Możesz wybrać predefiniowany szablon reguły, klikając odnośnik **Wybierz szablon**. Szablony reguły opisują najczęściej używane połączenia sieciowe.
Wszystkie ustawienia reguły sieciowej zostaną uzupełnione automatycznie.
17. Jeżeli chcesz, żeby działania reguły sieciowej były zapisywane w [raporcie](#), zaznacz pole **Zapisuj zdarzenia**.
18. Kliknij przycisk **Zapisz**.
Nowa reguła sieciowa zostanie dodana do listy.

19. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły sieciowej.


20. Zapisz swoje zmiany.

Ustawienia reguły sieciowej dla aplikacji

Parametr	Opis
Akcja	Zezwól. Blokuj.
Protokół	Kontroluj aktywność sieciową poprzez wybrany protokół: TCP, UDP, ICMP, ICMPv6, IGMP i GRE. Jeśli wybrałeś protokół ICMP lub ICMPv6, możesz zdefiniować typ i kod pakietu ICMP. Jeżeli jako typ protokołu wybrałeś TCP lub UDP, możesz określić porty komputera lokalnego oraz komputera zdalnego (rozdzielając je przecinkami), między którymi połączenie będzie monitorowane.
Kierunek	Przychodzący. Przychodzący / Wychodzący. Wychodzący.
Adresy zdalne	Adresy sieciowe zdalnych komputerów, które mogą wysyłać i/lub odbierać pakiety sieciowe. Zapora sieciowa stosuje regułę sieciową do określonego zakresu zdalnych adresów sieciowych. Możesz włączyć wszystkie adresy IP do reguły sieciowej, utworzyć oddzielną listę adresów IP, określić zakres adresów IP lub wybrać podsieć (Sieci zaufane, Sieci lokalne, Sieci publiczne). Możesz także określić nazwę DNS komputera zamiast jego adresu IP. Powinieneś używać nazw DNS tylko dla komputerów LAN lub wewnętrznych usług. Interakcja z usługami chmury (takimi jak Microsoft Azure) i innymi zasobami internetowymi powinna być zarządzana przez komponent Kontrola sieci.
Adresy lokalne	Adresy sieciowe komputerów, które mogą wysyłać i odbierać pakiety sieciowe. Zapora sieciowa stosuje regułę sieciową do określonego zakresu lokalnych adresów sieciowych. Możesz włączyć wszystkie adresy IP do reguły sieciowej, utworzyć oddzielną listę adresów IP lub określić zakres adresów IP. Możesz także określić nazwę DNS komputera zamiast jego adresu IP. Powinieneś używać nazw DNS tylko dla komputerów LAN lub wewnętrznych usług. Interakcja z usługami chmury (takimi jak Microsoft Azure) i innymi zasobami internetowymi powinna być zarządzana przez komponent Kontrola sieci. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;">Zdarza się, że dla aplikacji nie można uzyskać adresu lokalnego. W takim przypadku ten parametr jest ignorowany.</div>

Włączanie i wyłączanie reguły sieciowej dla aplikacji

W celu włączenia lub wyłączenia reguły sieciowej dla aplikacji:


1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij przycisk **Reguły aplikacji**.
Spowoduje to otwarcie listy reguł aplikacji.

4. Na liście aplikacji wybierz aplikację lub grupę aplikacji, dla której chcesz utworzyć lub zmodyfikować regułę sieciową.
5. Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Szczegóły i reguły**.
Zostanie otwarte okno właściwości i reguł aplikacji.
6. Zaznacz zakładkę **Reguły sieciowe**.
7. Na liście reguł sieciowych dla grupy aplikacji wybierz wymaganą regułę sieciową.
Zostanie otwarte okno właściwości reguły sieciowej.
8. Ustaw stan **Aktywny** lub **Nieaktywny** dla reguły sieciowej.
Nie możesz wyłączyć reguły sieciowej dla grupy aplikacji utworzonej domyślnie przez Zaporę sieciową.
9. Zapisz swoje zmiany.

Zmianianie akcji Zapory sieciowej dla reguły sieciowej dla aplikacji

Możesz zmienić akcję Zapory sieciowej stosowaną do wszystkich domyślnie utworzonych reguł sieciowych dla aplikacji lub grupy aplikacji, a także możesz zmienić akcję Zapory sieciowej stosowaną do pojedynczej niestandardowej reguły sieciowej dla aplikacji lub grupy aplikacji.

W celu zmiany akcji Zapory sieciowej stosowanej do wszystkich reguł sieciowych dla aplikacji lub grupy aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij przycisk **Reguły aplikacji**.
Spowoduje to otwarcie listy reguł aplikacji.
4. Jeśli chcesz zmienić akcję Zapory sieciowej, która jest stosowana do wszystkich domyślnie utworzonych reguł sieciowych, na liście wybierz aplikację lub grupę aplikacji. Ręcznie utworzone reguły sieciowe pozostają niezmienione.
5. Kliknij prawym klawiszem myszy i z otwartego menu kontekstowego wybierz **Reguły sieciowe**, a następnie wybierz działanie, które chcesz przypisać:
 - **Dziedzicz**.
 - **Zezwól**.
 - **Blokuj**.
6. Zapisz swoje zmiany.

W celu zmiany odpowiedzi Zapory sieciowej dla reguły sieciowej dla aplikacji lub grupy aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.

3. Kliknij przycisk **Reguły aplikacji**.
Spowoduje to otwarcie listy reguł aplikacji.
4. Na liście wybierz aplikację lub grupę aplikacji, dla której chcesz zmienić regułę sieciową.
5. Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Szczegóły i reguły**.
Zostanie otwarte okno właściwości i reguł aplikacji.
6. Zaznacz zakładkę **Reguły sieciowe**.
7. Wybierz regułę sieciową, dla której chcesz zmienić działanie Zapory sieciowej.
8. Kliknij prawym przyciskiem myszy kolumnę **Pozwolenie** i z otwartego menu kontekstowego wybierz akcję, którą chcesz przypisać:
 - **Dziedzicz.**
 - **Zezwól.**
 - **Blokuj.**
 - **Zapisuj zdarzenia.**
9. Zapisz swoje zmiany.


Zmienianie priorytetu reguły sieciowej dla aplikacji

Priorytet reguły sieciowej zależy od jej pozycji na liście reguł sieciowych. Zapora sieciowa wykonuje reguły w kolejności, w jakiej występują na liście reguł sieciowych (od góry do dołu). Zgodnie z każdą przetworzoną regułą sieciową, która odpowiada określonej połączeniu sieciowemu, Zapora sieciowa zezwala na lub blokuje dostęp sieciowy do adresu i portu określonego w ustawieniach tego połączenia sieciowego.

Ręcznie utworzone reguły sieciowe mają wyższy priorytet niż domyślne reguły sieciowe.

Nie można zmieniać priorytetu domyślnie utworzonych reguł sieciowych dla grupy aplikacji.

W celu zmiany priorytetu reguły sieciowej:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Zapora sieciowa**.
3. Kliknij przycisk **Reguły aplikacji**.
Spowoduje to otwarcie listy reguł aplikacji.
4. Na liście aplikacji wybierz aplikację lub grupę aplikacji, dla której chcesz zmienić priorytet reguły sieciowej.
5. Kliknij plik prawym przyciskiem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Szczegóły i reguły**.
Zostanie otwarte okno właściwości i reguł aplikacji.
6. Zaznacz zakładkę **Reguły sieciowe**.

- Wybierz regułę sieciową, której priorytet chcesz zmienić.
- Użyj przycisków **W górę** i **W dół**, aby przesunąć regułę sieciową na żądaną pozycję na liście.
- Zapisz swoje zmiany.

Monitor sieci

Monitor sieci to narzędzie służące do wyświetlania informacji o aktywności sieciowej komputera użytkownika w czasie rzeczywistym.

W celu uruchomienia Monitora sieci:

W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Monitor sieci**.

Zostanie otwarte okno **Monitor sieci**. W tym oknie informacje o aktywności sieciowej komputera są wyświetlane na czterech zakładkach:

- Zakładka **Aktywność sieciowa** wyświetla wszystkie aktualnie aktywne połączenia sieciowe komputera. Wyświetlane są połączenia przychodzące i wychodzące. Na tej zakładce możesz także [utworzyć reguły pakietów sieciowych](#) do działania Zapory sieciowej.
- Na zakładce **Otwarte porty** wyświetlane są wszystkie otwarte porty sieciowe komputera. Na tej zakładce możesz także [utworzyć reguły pakietów sieciowych](#) i [reguły aplikacji](#) do działania Zapory sieciowej.
- Zakładka **Ruch sieciowy** zawiera informacje dotyczące ilości wychodzącego i przychodzącego ruchu sieciowego między komputerem użytkownika a innymi komputerami w sieci, do której aktualnie podłączony jest użytkownik.
- Na zakładce **Zablokowane komputery** wyświetlane są adresy IP zdalnych komputerów, których aktywność sieciowa została zablokowana przez moduł Ochrona sieci po wykryciu prób ataków sieciowych pochodzących z tych adresów IP.

Ochrona przed atakami BadUSB

Niektóre wirusy modyfikują oprogramowanie wbudowane urządzeń USB w celu zmylenia systemu operacyjnego do wykrywania urządzenia USB jako klawiatury. W wyniku tego działania wirus może wykonać polecenia z poziomu konta użytkownika, na przykład, w celu pobrania szkodliwego oprogramowania.

Komponent Ochrona przed atakami BadUSB zapobiega podłączeniu do komputera zainfekowanych urządzeń USB emulujących klawiaturę.

Po podłączeniu urządzenia USB do komputera i zidentyfikowaniu go przez system operacyjny jako klawiatury, aplikacja wyświetli pytanie o wprowadzenie kodu numerycznego, wygenerowanego przez aplikację, z poziomu tej klawiatury lub [Klawiatury ekranowej, jeśli jest dostępna](#) (patrz rysunek poniżej). Ta procedura jest znana jako autoryzacja klawiatury.

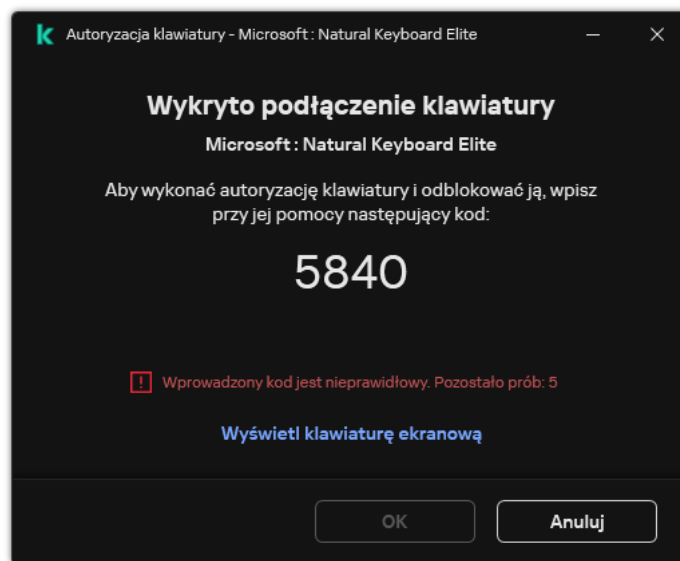
Jeśli kod zostanie wprowadzony poprawnie, aplikacja zapisze na liście zautoryzowanych klawiatur parametry identyfikujące klawiaturę - numer VID/PID, a także numer portu, do którego ta klawiatura została podpięta. Po ponownym podłączeniu klawiatury lub po ponownym uruchomieniu systemu nie ma konieczności powtarzania procesu autoryzacji klawiatury.

Jeśli zautoryzowana klawiatura zostanie podłączona do innego portu USB, aplikacja ponownie wyświetli pytanie o przeprowadzenie autoryzacji tej klawiatury.

Jeśli kod numeryczny zostanie wprowadzony niepoprawnie, aplikacja wygeneruje nowy kod. Możesz [skonfigurować liczbę prób wprowadzenia kodu numerycznego](#). Jeśli kod numeryczny zostanie wprowadzony niepoprawnie kilka razy lub okno autoryzacji klawiatury jest zamknięte (patrz rysunek poniżej), aplikacja zablokuje wprowadzenie z poziomu tej klawiatury. Po upływie czasu blokowania urządzenia USB lub ponownym uruchomieniu systemu operacyjnego, aplikacja ponownie wyświetli pytanie o przeprowadzenie autoryzacji klawiatury.

Aplikacja zezwoli na użycie zautoryzowanej klawiatury, a zablokuje klawiaturę, która nie została zautoryzowana.

Komponent Ochrona przed atakami BadUSB nie jest domyślnie instalowany. Jeśli potrzebujesz składnika Ochrona przed atakami BadUSB, możesz dodać ten składnik we właściwościach [pakietu instalacyjnego](#) przed zainstalowaniem aplikacji lub [zmienić dostępne składniki aplikacji](#) po zainstalowaniu aplikacji.




Autoryzacja klawiatury

Włączanie i wyłączanie Ochrony przed atakami BadUSB

Urządzenia USB, rozpoznawane przez system operacyjny jako klawiatury i podłączone do komputera przed zainstalowaniem modułu Ochrona przed atakami BadUSB, zostają uznane za zautoryzowane po zainstalowaniu modułu Ochrona przed atakami BadUSB.

W celu włączenia lub wyłączenia Ochrony przed atakami BadUSB:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona przed atakami BadUSB**.
3. Użyj przełącznika **Ochrona przed atakami BadUSB**, aby włączyć lub wyłączyć komponent.
4. W sekcji **Autoryzacja urządzeń USB** dostosuj ustawienia ochrony wprowadzania kodu autoryzacyjnego:

- **Maksymalna liczba prób autoryzacji urządzenia USB.** Automatyczne blokowanie urządzenia USB, jeśli kod autoryzacyjny jest wprowadzany niepoprawnie określoną liczbę. Ważne wartości to 1 do 10. Na przykład, jeśli zezwolisz na 5 prób wprowadzenia kodu autoryzacyjnego, urządzenie USB zostanie zablokowane po piątej nieudanej próbie. Kaspersky Endpoint Security wyświetla czas blokowania dla urządzenia USB. Po upływie tego czasu możesz mieć 5 prób wprowadzenia kodu autoryzacyjnego.
- **Limit czasu po osiągnięciu maksymalnej liczby prób (minuty).** Czas blokowania urządzenia USB po określonej liczbie nieudanych prób wprowadzenia kodu autoryzacyjnego. Ważne wartości to 1 do 180 (minuty).


5. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Ochrona przed atakami BadUSB jest włączona, Kaspersky Endpoint Security wymaga autoryzacji podłączonego urządzenia USB zidentyfikowanego przez system operacyjny jako klawiatura. Użytkownik może użyć niezautoryzowaną klawiaturę dopiero po jej zautoryzowaniu.

Korzystanie z Klawiatury ekranowej do autoryzacji urządzeń USB

Klawiatura ekranowa powinna być używana tylko do autoryzacji urządzeń USB, które nie obsługują wprowadzania losowych znaków (np. czytniki kodów kreskowych). Nie jest zalecane korzystanie z Klawiatury ekranowej do autoryzacji nieznanych urządzeń USB.

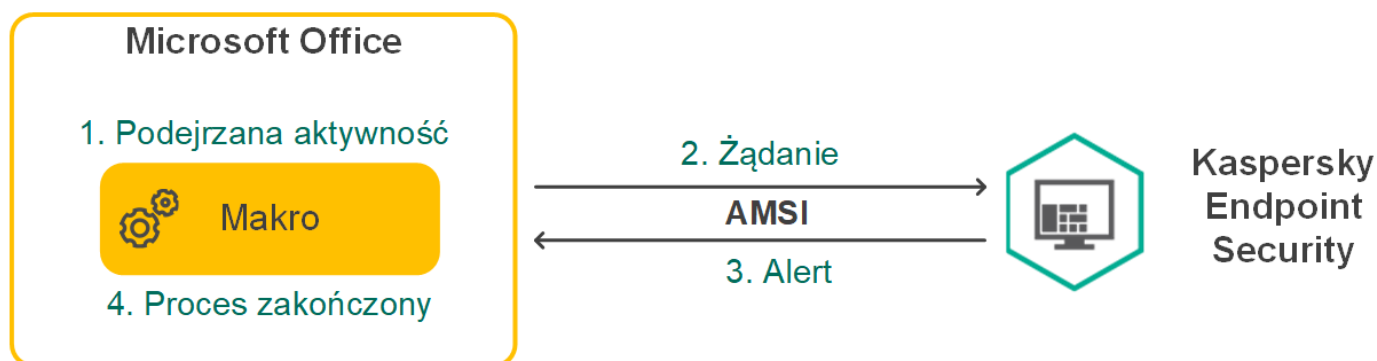
W celu zezwolenia na lub zablokowania użycia Klawiatury ekranowej do autoryzacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona przed atakami BadUSB**.
3. Aby zablokować lub zezwolić na użycie Klawiatury ekranowej do autoryzacji, użyj pola **Zabroń korzystania z Klawiatury ekranowej do autoryzacji urządzeń USB**.
4. Zapisz swoje zmiany.

Ochrona AMSI

Komponent Ochrona AMSI jest przeznaczony do obsługi Antimalware Scan Interface firmy Microsoft. *Antimalware Scan Interface (AMSI)* umożliwia aplikacjom firm trzecich z obsługą AMSI wysyłanie obiektów (na przykład, skryptów PowerShell) do Kaspersky Endpoint Security w celu przeprowadzenia dodatkowego skanowania i otrzymania wyników ze skanowania tych obiektów. Aplikacje firm trzecich mogą obejmować, na przykład, aplikacje Microsoft Office (patrz rysunek poniżej). Więcej informacji na temat AMSI znajdziesz w [dokumentacji firmy Microsoft](#).

Ochrona AMSI może tylko wykrywać zagrożenia i informować aplikację firmy trzeciej o wykrytym zagrożeniu. Aplikacja firmy trzeciej po odebraniu powiadomienia o zagrożeniu nie zezwala na wykonanie szkodliwych działań (na przykład, kończy proces).



Przykład działania AMSI

Komponent Ochrona AMSI może odrzucić żądanie z aplikacji firmy trzeciej, na przykład, jeśli ta aplikacja przekracza maksymalną liczbę żądań w określonym przedziale czasu. Kaspersky Endpoint Security wyśle informacje o odrzuconym żądaniu z aplikacji firmy trzeciej do Serwera administracyjnego. Komponent Ochrona AMSI nie odrzuca żądań od tych aplikacji firm trzecich, dla których pole [Nie blokuj interakcji z modułem Ochrona AMSI](#) jest zaznaczone.


Ochrona AMSI jest dostępny dla następujących systemów operacyjnych dla stacji roboczych i serwerów:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows 11;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Włączanie i wyłączanie Ochrony AMSI

Domyślnie, moduł Ochrona AMSI jest włączony.


W celu włączenia lub wyłączenia modułu Ochrona AMSI:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona AMSI**.
3. Użyj przełącznika **Ochrona AMSI**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

Używanie Ochrony AMSI do skanowania plików złożonych

Popularną techniką ukrywania wirusów i innego szkodliwego oprogramowania jest osadzanie ich w plikach złożonych, takich jak archiwa. W celu wykrycia ukrytych w ten sposób wirusów i innego szkodliwego oprogramowania, plik złożony musi zostać rozpakowany, co może spowolnić skanowanie. Możesz ograniczyć typy skanowanych plików złożonych, dzięki czemu skanowanie będzie szybsze.

W celu skonfigurowania skanowania plików złożonych przez Ochronę AMSI:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Podstawowa ochrona przed zagrożeniami** → **Ochrona AMSI**.
3. W sekcji **Skanowanie plików złożonych** określ, które pliki złożone mają być skanowane: archiwa, pakiety instalacyjne lub pliki w formatach pakietu Office.
4. W sekcji **Ograniczenie rozmiaru** wykonaj jedną z poniższych czynności:
 - Aby moduł Ochrona AMSI nie rozpakowywał dużych plików złożonych, zaznacz pole **Nie rozpakowuj dużych plików złożonych** i określ żądaną wartość w polu **Maksymalny rozmiar pliku**. Komponent Ochrona AMSI nie będzie rozpakowywać plików złożonych, których rozmiar jest większy niż określona wartość.
 - Aby moduł Ochrona AMSI rozpakowywał duże pliki złożone, usuń zaznaczenie z pola **Nie rozpakowuj dużych plików złożonych**.

Komponent Ochrona AMSI skanuje duże pliki wypakowane z archiwów bez względu na to, czy pole **Nie rozpakowuj dużych plików złożonych** jest zaznaczone.

5. Zapisz swoje zmiany.


Ochrona przed exploitami

Komponent Ochrona przed exploitami wykrywa kod programu, który wykorzystuje luki na komputerze, aby użyć uprawnień administratora lub wykonać szkodliwe aktywności. Na przykład, exploit wysyła dużą ilość danych do aplikacji zawierającej lukę. Podczas przetwarzania tych danych aplikacja zawierająca lukę wykona szkodliwy kod. W wyniku tego ataku exploit może uruchomić nieautoryzowaną instalację szkodliwego programu. Po wykryciu, że próba uruchomienia pliku wykonywalnego z aplikacji zawierającej luki nie została zainicjowana przez użytkownika, Kaspersky Endpoint Security zablokuje uruchomienie tego pliku lub poinformuje użytkownika.

Włączanie i wyłączanie modułu Ochrona przed exploitami

Domyślnie moduł Ochrona przed exploitami jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. W razie konieczności możesz wyłączyć Ochronę przed exploitami.

W celu włączenia lub wyłączenia Ochrony przed exploitami:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed exploitami**.
3. Użyj przełącznika **Ochrona przed exploitami**, aby włączyć lub wyłączyć komponent.


4. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Ochrona przed exploitami jest włączona, Kaspersky Endpoint Security będzie monitorował pliki wykonywalne, które są uruchamiane przez aplikacje zawierające luki. Jeśli Kaspersky Endpoint Security wykryje, że plik wykonywalny z aplikacji zawierającej luki nie został uruchomiony przez użytkownika, Kaspersky Endpoint Security wykona wybraną akcję (na przykład, zablokuje działanie).

Wybieranie działania, jakie ma zostać wykonane po wykryciu exploita

Domyślnie, po wykryciu exploita, program Kaspersky Endpoint Security blokuje działania, które exploit próbuje wykonać.


W celu wybrania działania, jakie ma zostać wykonane po wykryciu exploita:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed exploitami**.
3. W sekcji **Po wykryciu exploita** wybierz żądaną akcję:
 - **Zablokuj operację.** Jeśli ten element jest wybrany, po wykryciu exploita, Kaspersky Endpoint Security zablokuje działania tego exploita i zarejestruje w raporcie informacje o tym exploicie.
 - **Informuj.** Jeśli ten element jest wybrany, gdy Kaspersky Endpoint Security wykryje exploita, zarejestruje w raporcie informacje o exploicie i doda informacje o tym exploicie do listy aktywnych zagrożeń.
4. Zapisz swoje zmiany.

Ochrona pamięci procesów systemowych

Domyślnie ochrona pamięci procesów systemowych jest włączona.

W celu włączenia lub wyłączenia ochrony pamięci procesów systemowych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed exploitami**.
3. Użyj przełącznika **Włącz ochronę pamięci procesów systemowych**, aby włączyć lub wyłączyć tę funkcję.
4. Zapisz swoje zmiany.

W wyniku tego działania program Kaspersky Endpoint Security zablokuje zewnętrzne procesy, które próbują uzyskać dostęp do procesów systemowych.

Wykrywanie zachowań


Komponent Wykrywanie zachowań gromadzi dane na temat działań aplikacji na komputerze i dostarcza te informacje innym składnikom ochrony w celu udoskonalenia ich działania. Komponent Wykrywanie zachowań używa sygnatur strumieni zachowań (BSS) dla aplikacji. Jeśli aktywność aplikacji odpowiada sygnaturze strumienia zachowań, Kaspersky Endpoint Security wykona wybrane działanie. Funkcjonalność Kaspersky Endpoint Security oparta na sygnaturach strumieni zachowań zapewnia ochronę proaktywną komputera.

Włączanie i wyłączanie modułu Wykrywanie zachowań

Domyślnie moduł Wykrywanie zachowań jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky. W razie konieczności możesz wyłączyć Wykrywanie zachowań.

Nie jest zalecane wyłączanie modułu Wykrywanie zachowań, chyba że jest to faktycznie konieczne, gdyż może to zmniejszyć efektywność składników ochrony. Składniki ochrony mogą żądać danych zebranych przez komponent Wykrywanie zachowań do wykrywania zagrożeń.


W celu włączenia lub wyłączenia Wykrywania zachowań:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Wykrywanie zachowań**.
3. Użyj przełącznika **Wykrywanie zachowań**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Wykrywanie zachowań jest włączone, Kaspersky Endpoint Security będzie używał sygnatury strumieni zachowań do analizy aktywności aplikacji w systemie operacyjnym.

Wybieranie działania, jakie ma zostać podjęte po wykryciu szkodliwej aktywności

W celu wybrania akcji, jaka ma zostać wykonana, gdy aplikacja wykryje szkodliwą aktywność:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Wykrywanie zachowań**.
3. W sekcji **Po wykryciu aktywności szkodliwego oprogramowania** wybierz odpowiednią akcję:
 - **Usuń plik.** Jeśli ten element jest wybrany, po wykryciu szkodliwej aktywności program Kaspersky Endpoint Security usunie plik wykonywalny szkodliwej aplikacji i utworzy kopię zapasową pliku w Kopii zapasowej.
 - **Przerwij działanie aplikacji.** Jeśli wybrano ten element, po wykryciu szkodliwej aktywności Kaspersky Endpoint Security zakończy działanie tej aplikacji.
 - **Informuj.** Jeśli ten element jest wybrany i zostanie wykryta szkodliwa aktywność aplikacji, Kaspersky Endpoint Security doda informację o szkodliwej aktywności aplikacji do listy aktywnych zagrożeń.
4. Zapisz swoje zmiany.

Ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym

Komponent monitoruje operacje wykonywane tylko na tych plikach, które są przechowywane na urządzeniach pamięci masowej z systemem plików NTFS i które nie są zaszyfrowane za pomocą systemu szyfrowania EFS.

Ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym zapewnia analizę aktywności w folderach współdzielonych. Jeśli to działanie jest zgodne z sygnaturą strumieni zachowań, która jest typowa dla zewnętrznego szyfrowania, Kaspersky Endpoint Security wykonuje wybraną akcję.


Domyślnie, ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym jest wyłączona.

Po zainstalowaniu Kaspersky Endpoint Security, ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym zostanie ograniczona do momentu ponownego uruchomienia komputera.

Włączanie i wyłączanie ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym


Po zainstalowaniu Kaspersky Endpoint Security, ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym zostanie ograniczona do momentu ponownego uruchomienia komputera.

W celu włączenia ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Wykrywanie zachowań**.
3. Użyj przełącznika **Włącz ochronę folderów współdzielonych przed szyfrowaniem zewnętrznym**, aby włączyć lub wyłączyć wykrywanie aktywności typowej dla szyfrowania zewnętrznego.
4. Zapisz swoje zmiany.

Wybieranie działania, jakie ma zostać wykonane po wykryciu szyfrowania zewnętrznego folderów współdzielonych

W celu wybrania działania, jakie ma zostać wykonane po wykryciu szyfrowania zewnętrznego folderów współdzielonych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Wykrywanie zachowań**.
3. W sekcji **Ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym** wybierz żądaną akcję:

- **Blokuj połączenie przez N min.** Jeśli opcja została wybrana i Kaspersky Endpoint Security wykryje próbę zmodyfikowania plików w folderach współdzielonych, wykona następujące działania:
 - Zablokuje aktywność sieciową komputera podejmującego próbę modyfikacji.
 - Utworzy kopie zapasowe plików, które są modyfikowane.
 - Doda wpis do [lokalnych raportów dotyczących interfejsu aplikacji](#).
 - Wyśle informacje o wykrytej szkodliwej aktywności do Kaspersky Security Center.

Dodatkowo, jeśli komponent Silnik korygujący jest włączony, zmodyfikowane pliki zostają przywrócone z kopii zapasowych.

- **Informuj.** Jeśli opcja została wybrana i Kaspersky Endpoint Security wykryje próbę zmodyfikowania plików w folderach współdzielonych, wykona następujące działania:
 - Doda wpis do [lokalnych raportów dotyczących interfejsu aplikacji](#).
 - Doda wpis do listy aktywnych zagrożeń.
 - Wyśle informacje o wykrytej szkodliwej aktywności do Kaspersky Security Center.

4. Zapisz swoje zmiany.

W celu włączenia ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym:

Wykluczenie folderu może zmniejszyć liczbę fałszywych alarmów, jeśli Twoja organizacja używa szyfrowania danych podczas wymiany plików za pomocą folderów współdzielonych. Na przykład Wykrywanie zachowania może dawać fałszywe alarmy, gdy użytkownik pracuje z plikami z rozszerzeniem ENC w folderze współdzielonym. Takie działanie odpowiada wzorcowi zachowania, który jest typowy dla szyfrowania zewnętrznego. Jeśli w celu ochrony danych zaszyfrowałeś pliki w folderze współdzielonym, dodaj ten folder do wykluczeń.

[Jak utworzyć wykluczenie dla ochrony folderów współdzielonych za pomocą Konsoli administracyjnej.\(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Zasady**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Ustawienia ogólne** → **Wykluczenia**.
6. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** kliknij przycisk **Ustawienia**.
7. W otwartym oknie wybierz zakładkę **Wykluczenia ze skanowania**.
Zostanie otwarte okno zawierające listę wykluczeń.
8. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę wykluczeń dla wszystkich komputerów w firmie. Listy wykluczeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Wykluczenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie wykluczeń zasady nadrzędnej nie jest możliwe.
9. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy wykluczeń, zaznacz pole **Zezwól na korzystanie z lokalnych zaufanych aplikacji**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę wykluczeń jako dodatek do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Jeśli lokalna lista została wygenerowana, po wyłączeniu tej funkcjonalności program Kaspersky Endpoint Security kontynuuje wykluczenie listy plików ze skanowania.

10. Kliknij **Dodaj**.
11. W sekcji **Właściwości** zaznacz pole **Plik lub folder**.
12. Kliknij odnośnik **wybierz plik lub folder** w sekcji **Opis wykluczenia ze skanowania (kliknij podkreślone elementy, aby je zmodyfikować)**, aby otworzyć okno **Nazwa pliku lub folderu**.
13. Kliknij **Przełóżaj** i wybierz folder współdzielony.
Możesz również ręcznie wprowadzić ścieżkę. Kaspersky Endpoint Security obsługuje znaki * i ? podczas wprowadzania maski:
 - Znak * (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:**.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
 - Dwa występujące po sobie znaki * zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder**.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie Folder i w jego podfolderach. Maskę musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maskę C:***.txt nie jest ważną maską.

- Znak ? (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: \ i / (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder\???.txt będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie Folder, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

14. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.
15. Po kliknięciu odnośnika **dowolne** w sekcji **Opis wykluczenia ze skanowania (kliknij podkreślone elementy, aby je zmodyfikować)**, zostanie aktywowany odnośnik **wybierz moduły**.
16. Kliknięcie odnośnika **wybierz moduły** otwiera okno **Składniki ochrony**.
17. Zaznacz pole wyboru obok komponentu **Wykrywanie zachowania**.
18. Zapisz swoje zmiany.

[Jak utworzyć wykluczenie dla ochrony folderów współdzielonych za pomocą Web Console i Cloud Console](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia ogólne** → **Wykluczenia**.
5. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** kliknij odnośnik **Wykluczenia ze skanowania**.
6. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę wykluczeń dla wszystkich komputerów w firmie. Listy wykluczeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Wykluczenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie wykluczeń zasady nadrzędnej nie jest możliwe.
7. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy wykluczeń, zaznacz pole **Zezwól na korzystanie z lokalnych zaufanych aplikacji**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę wykluczeń jako dodatek do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Jeśli lokalna lista została wygenerowana, po wyłączeniu tej funkcjonalności program Kaspersky Endpoint Security kontynuuje wykluczenie listy plików ze skanowania.
8. Kliknij przycisk **Dodaj**.
9. Wybierz sposób dodania wykluczenia: **Plik lub folder**.
10. Kliknij **Przełóżnik** i wybierz folder współdzielony.


Możesz również ręcznie wprowadzić ścieżkę. Kaspersky Endpoint Security obsługuje znaki * i ? podczas wprowadzania maski.
 - Znak * (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:**.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
 - Dwa występujące po sobie znaki * zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder***.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie Folder i w jego podfolderach. Maskę musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maskę C:***.txt nie jest ważną maską.
 - Znak ? (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder\???.txt będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie Folder, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.
11. W sekcji **Składniki ochrony** zaznacz komponent **Wykrywanie zachowań**.
12. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

13. Dla wykluczenia wybierz stan **Aktywny**.

W dowolnym momencie możesz użyć przełącznika do [zatrzymania wykluczenia](#).

14. Zapisz swoje zmiany.

[Jak utworzyć wykluczenie dla ochrony folderów współdzielonych w interfejsie aplikacji](#)

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Ustawienia ogólne** → **Zagrożenia i wykluczenia**.

3. W sekcji **Wykluczenia** kliknij odnośnik **Zarządzaj wykluczeniami**.

4. Kliknij **Dodaj**.

5. Kliknij **Przeglądaj** i wybierz folder współdzielony.

Możesz również ręcznie wprowadzić ścieżkę. Kaspersky Endpoint Security obsługuje znaki * i ? podczas wprowadzania maski.

- Znak * (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:**.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
- Dwa występujące po sobie znaki * zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder***.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie Folder i w jego podfolderach. Maski musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maski C:***.txt nie jest ważną maską.
- Znak ? (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder\???.txt będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie Folder, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

6. W sekcji **Składniki ochrony** zaznacz pole **Wykrywanie zachowań**.

7. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

8. Dla wykluczenia wybierz stan **Aktywny**.

W dowolnym momencie możesz użyć przełącznika do [zatrzymania wykluczenia](#).


9. Zapisz swoje zmiany.

Konfigurowanie adresów komputerów dla wykluczeń z ochrony folderów współdzielonych przed szyfrowaniem zewnętrznym

Aby możliwe było wyłączenie wykluczeń adresów z ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem, musi być włączona usługa Przeprowadź inspekcję logowania. Domyślnie, usługa Przeprowadź inspekcję logowania jest wyłączona (szczegółowe informacje dotyczące włączania usługi Przeprowadź inspekcję logowania można znaleźć na stronie internetowej firmy Microsoft).

Funkcjonalność wykluczania adresów z ochrony folderów sieciowych nie działa na zdalnym komputerze, jeśli zdalny komputer został włączony przed uruchomieniem Kaspersky Endpoint Security. Możesz ponownie uruchomić ten zdalny komputer po uruchomieniu Kaspersky Endpoint Security, aby upewnić się, że funkcjonalność wykluczania adresów z ochrony folderów współdzielonych działa na tym zdalnym komputerze.

W celu wykluczenia zdalnych komputerów, które wykonują zdalne szyfrowanie folderów współdzielonych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Wykrywanie zachowań**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Konfiguruj wykluczone adresy**.
4. Jeśli chcesz dodać adres IP lub nazwę komputera do listy wykluczeń, kliknij przycisk **Dodaj**.
5. Wprowadź adres IP lub nazwę komputera, z którego próby zewnętrznego szyfrowania nie muszą być zatrzymywane.
6. Zapisz swoje zmiany.

Eksportowanie i importowanie listy wykluczeń z ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem

Możesz wyeksportować listę wykluczeń do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę adresów tego samego typu. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy wykluczeń lub przeniesienia listy na inny serwer.

[Eksportowanie i importowanie listy wykluczeń w Konsoli administracyjnej \(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Wykrywanie zachowań**.
6. W sekcji **Ochrona folderów współdzielonych przed szyfrowaniem zewnętrznym** kliknij przycisk **Wykluczenia**.
7. W celu wyeksportowania listy reguł:
 - a. Wybierz wykluczenia, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

Jeśli nie wybrałeś żadnego wykluczenia, Kaspersky Endpoint Security wyeksportuje wszystkie wykluczenia.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.

Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML.
8. W celu zaimportowania listy wykluczeń:
 - a. Kliknij przycisk **Importuj**.
 - b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.
 - c. Kliknij przycisk **Otwórz**.

Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
9. Zapisz swoje zmiany.

[Eksportowanie i importowanie listy wykluczeń w Web Console i Cloud Console](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listę wykluczeń.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Wykrywanie zachowań**.
5. W celu wyeksportowania listy wykluczeń w sekcji **Wykluczenia**:
 - a. Wybierz wykluczenia, które chcesz wyeksportować.
 - b. Kliknij przycisk **Eksportuj**.
 - c. Potwierdź chęć wyeksportowania tylko wybranych wykluczeń lub wyeksportuj całą listę wykluczeń.
 - d. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
 - e. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML.
6. W celu zaimportowania listy wykluczeń w sekcji **Wykluczenia**:
 - a. Kliknij przycisk **Importuj**.
 - b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.
 - c. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
7. Zapisz swoje zmiany.

Ochrona przed włamaniami

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Ochrona przed włamaniami uniemożliwia aplikacjom wykonywanie działań niebezpiecznych dla systemu operacyjnego i zapewnia kontrolę dostępu do zasobów systemu operacyjnego i danych osobowych. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network.

Komponent kontroluje działanie aplikacji za pomocą *uprawnień aplikacji*. Uprawnienia aplikacji obejmują następujące parametry dostępu:

- Dostęp do zasobów systemu operacyjnego (na przykład opcje automatycznego uruchamiania, klucze rejestru)
- Dostęp do danych osobowych (takich jak pliki i aplikacje)

Aktywność sieciowa aplikacji jest kontrolowana przez [Zaporę sieciową](#) za pomocą *reguł sieciowych*.

Podczas pierwszego uruchomienia aplikacji Ochrona przed włamaniami wykonuje następujące działania:

1. Sprawdza bezpieczeństwo aplikacji przy użyciu pobranych antywirusowych baz danych.
2. Sprawdza bezpieczeństwo aplikacji w Kaspersky Security Network.

Zalecane jest [uczestniczenie w Kaspersky Security Network](#), aby zapewnić bardziej efektywne działanie komponentu Ochrona przed włamaniami.

3. Umieszcza aplikację w jednej z *grup zaufania*: Zaufane, Niski poziom ograniczeń, Wysoki poziom ograniczeń, Niezaufane.

[Grupa zaufania określa uprawnienia](#), do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.

Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania dla składników Zapora sieciowa i Ochrona przed włamaniami. Nie można zmienić grupy zaufania tylko dla Zapory sieciowej lub Ochrony przed włamaniami.

Jeśli odmówiłeś uczestnictwa w KSN lub nie ma sieci, Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od [ustawień modułu Ochrona przed włamaniami](#). Po otrzymaniu reputacji aplikacji od KSN, grupę zaufania można zmienić automatycznie.

4. Blokuje działania aplikacji w zależności od grupy zaufania. Na przykład, aplikacje z grupy Wysoki poziom ograniczeń mają zablokowany dostęp do modułów systemu operacyjnego.

Przy następnym uruchomieniu aplikacji, Kaspersky Endpoint Security sprawdzi integralność aplikacji. Jeżeli aplikacja nie została zmieniona, moduł użyje dla niej bieżących uprawnień aplikacji. Jeżeli aplikacja została zmodyfikowana, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

Włączanie i wyłączenie modułu Ochrona przed włamaniami

Domyślnie moduł Ochrona przed włamaniami jest włączony i działa w trybie zalecanym przez ekspertów z Kaspersky.


[Jak włączyć lub wyłączyć komponent Ochrona przed włamaniami w Konsoli administracyjnej.\(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
6. Użyj pola **Ochrona przed włamaniami**, aby włączyć lub wyłączyć komponent.
7. Zapisz swoje zmiany.

[Jak włączyć lub wyłączyć komponent Ochrona przed włamaniami w Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
5. Użyj przełącznika **Ochrona przed włamaniami**, aby włączyć lub wyłączyć komponent.
6. Zapisz swoje zmiany.

[Jak włączyć lub wyłączyć komponent Ochrona przed włamaniami w interfejsie aplikacji?](#)

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. Użyj przełącznika **Ochrona przed włamaniami**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

Jeśli komponent Ochrona przed włamaniami jest włączona, Kaspersky Endpoint Security umieszcza aplikację w [grupie zaufania](#), w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera. Następnie Kaspersky Endpoint Security zablokuje działania aplikacji w zależności od grupy zaufania.

Zarządzanie grupami zaufania aplikacji

Przy pierwszym uruchomieniu aplikacji moduł Ochrona przed włamaniami sprawdza jej bezpieczeństwo i umieszcza w [grupie zaufania](#).

W pierwszym kroku skanowania aplikacji Kaspersky Endpoint Security przeszukuje wewnętrzną bazę danych znanych aplikacji w poszukiwaniu odpowiadającego jej wpisu i jednocześnie wysyła żądanie do bazy danych Kaspersky Security Network (jeśli dostępne jest połączenie internetowe). W oparciu o wyniki przeszukiwania wewnętrznej bazy danych i bazy danych Kaspersky Security Network, aplikacja zostaje umieszczona w grupie zaufania. Przy każdym kolejnym uruchomieniu aplikacji program Kaspersky Endpoint Security wysyła nowe zapytanie do bazy danych KSN i umieszcza aplikację w innej grupie zaufania, jeśli reputacja aplikacji w bazie danych KSN uległa zmianie.

Możesz wybrać grupę zaufania, do której program Kaspersky Endpoint Security musi [automatycznie przypisać wszystkie nieznanne aplikacje](#). Aplikacje, które zostały uruchomione przed Kaspersky Endpoint Security, są automatycznie przenoszone do grupy zaufania [Ustawienia modułu Ochrona przed włamaniami](#).

Dla aplikacji, które zostały uruchomione przed Kaspersky Endpoint Security, kontrolowana jest tylko aktywność sieciowa. Kontrola odbywa się zgodnie z regułami sieciowymi [określonymi w ustawieniach Zapory sieciowej](#).

Zmiana grupy zaufania aplikacji

Przy pierwszym uruchomieniu aplikacji moduł Ochrona przed włamaniami sprawdza jej bezpieczeństwo i umieszcza w [grupie zaufania](#).

Specjaliści z Kaspersky nie zalecają przenoszenia aplikacji z automatycznie przydzielonej grupy zaufania do innej grupy zaufania. Zamiast tego możesz [zmodyfikować uprawnienia dla pojedynczej aplikacji](#) (jeśli to konieczne).


[Jak zmienić grupę zaufania aplikacji w Konsoli administracyjnej \(MMC\)?](#) 


1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
6. W sekcji **Reguły kontroli aplikacji oraz chronionych zasobów** kliknij **Ustawienia**.
To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
7. Wybierz zakładkę **Uprawnienia aplikacji**.
8. Kliknij przycisk **Dodaj**.
9. W otwartym oknie wprowadź kryteria wyszukiwania aplikacji, której grupę zaufania chcesz zmienić.
Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki ***** i **?**.
10. Kliknij przycisk **Odśwież**.
Kaspersky Endpoint Security wyszuka aplikację na skonsolidowanej liście aplikacji zainstalowanych na zarządzanych komputerach. Kaspersky Endpoint Security wyświetli listę aplikacji spełniających Twoje kryteria wyszukiwania.
11. Wybierz żadaną aplikację.
12. Z listy rozwijalnej **Dodaj wybraną aplikację do grupy zaufania** wybierz żadaną grupę zaufania dla aplikacji.
13. Zapisz swoje zmiany.

[Jak zmienić grupę zaufania aplikacji w Web Console i Cloud Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
5. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij odnośnik **Uprawnienia aplikacji i zasoby chronione**.
To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
6. Wybierz zakładkę **Uprawnienia aplikacji**.
W lewej części okna zobaczysz listę grup zaufania, a w prawej części okna zobaczysz i ich właściwości.
7. Kliknij przycisk **Dodaj**.
To spowoduje uruchomienie Kreatora dodawania aplikacji do grupy zaufania.
8. Wybierz odpowiednią grupę zaufania dla aplikacji.
9. Wybierz typ **Aplikacja**. Kliknij przycisk **Dalej**.
Jeśli chcesz zmienić grupę zaufania dla kilku aplikacji, wybierz typ **Grupa** i określ nazwę grupy zaufania.
10. Z otwartej listy aplikacji wybierz aplikacje, dla których chcesz zmienić grupę zaufania.
Użyj filtra. Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki * i ?.
11. Zakończ działanie kreatora, klikając **OK**.
Aplikacja zostanie dodana do grupy zaufania.
12. Zapisz swoje zmiany.

[Jak zmienić grupę zaufania aplikacji w interfejsie aplikacji?](#)

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. Kliknij przycisk **Zarządzaj aplikacjami**.
Spowoduje to otwarcie listy zainstalowanych aplikacji.
4. Wybierz żadaną aplikację.
5. Z menu kontekstowego aplikacji wybierz **Ograniczenia** → **<grupa zaufania>**.
6. Zapisz swoje zmiany.

W wyniku tego działania aplikacja zostanie umieszczona w innej grupie zaufania. Następnie Kaspersky Endpoint Security zablokuje działania aplikacji w zależności od grupy zaufania. Stan  (zdefiniowany przez użytkownika) zostanie przypisany do aplikacji. Jeśli reputacja aplikacji została zmieniona w Kaspersky Security Network, Ochrona przed włamaniami pozostawi tę grupę zaufania aplikacji niezmienną.

Konfigurowanie uprawnień grupy zaufania

[Optymalne uprawnienia aplikacji](#) są domyślnie tworzone dla różnych grup zaufania. Ustawienia uprawnień dla grup aplikacji, które nie znajdują się w grupie zaufania, dziedziczą wartości z ustawień uprawnień grupy zaufania.


[Jak zmienić uprawnienia grupy zaufania w Konsoli administracyjnej.\(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
 2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
 3. W obszarze roboczym wybierz zakładkę **Profile**.
 4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
 5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
 6. W sekcji **Reguły kontroli aplikacji oraz chronionych zasobów** kliknij **Ustawienia**.
To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
 7. Wybierz zakładkę **Uprawnienia aplikacji**.
 8. Wybierz żądaną grupę zaufania.
 9. Wybierz **Uprawnienia grupy** z menu kontekstowego grupy zaufania.
Spowoduje to otwarcie właściwości grupy zaufania.
 10. Wykonaj jedną z poniższych czynności:
 - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz zakładkę **Pliki i rejestr systemu**.
 - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz zakładkę **Uprawnienia**.
- Aktywność sieciowa aplikacji jest kontrolowana przez [Zaporę sieciową](#) za pomocą *reguł sieciowych*.
11. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania kliknij je prawym klawiszem myszy, aby otworzyć menu kontekstowe i wybrać odpowiednią opcję: **Dziedzicz**, **Zezwól** (✓) lub **Zablokuj** (⊘).
 12. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** (✓ / ⊘).
Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.
 13. Zapisz swoje zmiany.




[Jak zmienić uprawnienia grupy zaufania w Web Console i Cloud Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
 2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
 3. Wybierz zakładkę **Ustawienia aplikacji**.
 4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
 5. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij odnośnik **Uprawnienia aplikacji i zasoby chronione**.
To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
 6. Wybierz zakładkę **Uprawnienia aplikacji**.
W lewej części okna zobaczysz listę grup zaufania, a w prawej części okna zobaczysz ich właściwości.
 7. W lewej części okna wybierz odpowiednią grupę zaufania.
 8. W prawej części okna, z listy rozwijalnej wykonaj jedną z następujących czynności:
 - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz **Pliki i rejestr systemu**.
 - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz **Uprawnienia**.
- Aktywność sieciowa aplikacji jest kontrolowana przez [Zaporę sieciową](#) za pomocą *reguł sieciowych*.
9. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania wybierz odpowiednią opcję: **Dziedzicz**, **Zezwól** (✔) lub **Zablokuj** (✘).
 10. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** (✔ / ✘).
Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.
 11. Zapisz swoje zmiany.

[Jak zmienić uprawnienia grupy zaufania w interfejsie aplikacji?](#) 

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. Kliknij przycisk **Zarządzaj aplikacjami**.
Spowoduje to otwarcie listy zainstalowanych aplikacji.
4. Wybierz żadaną grupę zaufania.
5. Z menu kontekstowego grupy zaufania wybierz **Szczegóły i reguły**.
Spowoduje to otwarcie właściwości grupy zaufania.
6. Wykonaj jedną z poniższych czynności:
 - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz zakładkę **Pliki i rejestr systemu**.
 - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz zakładkę **Uprawnienia**.

Aktywność sieciowa aplikacji jest kontrolowana przez [Zaporę sieciową](#) za pomocą *reguł sieciowych*.

7. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania kliknij je prawym klawiszem myszy, aby otworzyć menu kontekstowe i wybrać odpowiednią opcję: **Dziedzicz**, **Zezwól**  lub **Zablokuj** .
8. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** .
Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacjach, które używają każdego zasobu.
9. Zapisz swoje zmiany.

Uprawnienia grupy zaufania zostaną zmienione. Następnie Kaspersky Endpoint Security zablokuje działania aplikacji w zależności od grupy zaufania. Stan  (*Ustawienia użytkownika*) zostanie przypisany do grupy zaufania.

Wybieranie grupy zaufania dla aplikacji uruchamianych przed Kaspersky Endpoint Security

Dla aplikacji, które zostały uruchomione przed Kaspersky Endpoint Security, kontrolowana jest tylko aktywność sieciowa. Kontrola odbywa się zgodnie z [regułami sieciowymi](#) określonymi w ustawieniach Zapory sieciowej. Aby określić, które reguły sieciowe muszą być stosowane do monitorowania aktywności sieciowej dla tych aplikacji, należy wybrać grupę zaufania.


[Jak wybrać grupę zaufania dla aplikacji uruchomionych przed Kaspersky Endpoint Security w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
6. W sekcji **Uprawnienia aplikacji** kliknij przycisk **Edytuj**.
7. Dla ustawienia **Grupa zaufania dla aplikacji uruchamianych zanim Kaspersky Endpoint Security for Windows zacznie działać** wybierz odpowiednią [grupę zaufania](#).
8. Zapisz swoje zmiany.

[Jak wybrać grupę zaufania dla aplikacji uruchomionych przed Kaspersky Endpoint Security w Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
5. Dla ustawienia **Grupa zaufania dla aplikacji uruchamianych zanim Kaspersky Endpoint Security for Windows zacznie działać** wybierz odpowiednią [grupę zaufania](#).
6. Zapisz swoje zmiany.

[Jak wybrać grupę zaufania dla aplikacji uruchomionych przed Kaspersky Endpoint Security w interfejsie aplikacji?](#)

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. Dla ustawienia **Grupa zaufania dla aplikacji uruchamianych zanim Kaspersky Endpoint Security for Windows zacznie działać** wybierz odpowiednią [grupę zaufania](#).
4. Zapisz swoje zmiany.

W wyniku tego działania aplikacja, która jest uruchamiana przed Kaspersky Endpoint Security, zostanie umieszczona w innej grupie zaufania. Następnie Kaspersky Endpoint Security zablokuje działania aplikacji w zależności od grupy zaufania.

Wybieranie grupy zaufania dla nieznanymi aplikacji

Podczas pierwszego uruchomienia aplikacji komponent Ochrona przed włamaniami określa [grupę zaufania](#) dla aplikacji. Jeśli nie masz dostępu do internetu lub jeśli Kaspersky Security Network nie zawiera informacji o tej aplikacji, domyślnie Kaspersky Endpoint Security umieści aplikację w grupie Ograniczenia niskiego poziomu. Jeśli informacje o wcześniej nieznanymi aplikacji zostały wykryte w KSN, Kaspersky Endpoint Security zaktualizuje uprawnienia tej aplikacji. Następnie możesz [ręcznie edytować uprawnienia aplikacji](#).


[Jak wybrać grupę zaufania dla nieznanymi aplikacji w Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
6. W sekcji **Reguły działania aplikacji** użyj listy rozwijalnej **Grupa zaufania dla aplikacji, których nie można dodać do istniejących grup**, aby wybrać żądaną grupę zaufania.
Jeśli uczestnictwo w [Kaspersky Security Network jest włączone](#), Kaspersky Endpoint Security wysła do KSN pytanie odnośnie reputacji aplikacji za każdym razem, gdy jest ona uruchamiana. W oparciu o uzyskaną odpowiedź, aplikacja może zostać przeniesiona do grupy zaufania, która jest inna niż ta określona w ustawienia komponentu Ochrona przed włamaniami.
7. Użyj pola **Aktualizuj uprawnienia dla wcześniej nieznanymi aplikacji z bazy danych KSN**, aby skonfigurować automatyczną aktualizację uprawnień nieznanymi aplikacji.
8. Zapisz swoje zmiany.

[Jak wybrać grupę zaufania dla nieznanymi aplikacji w Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
5. W sekcji **Reguły działania aplikacji** użyj listy rozwijalnej **Grupa zaufania dla aplikacji, których nie można dodać do istniejących grup**, aby wybrać żadaną grupę zaufania.
Jeśli uczestnictwo w [Kaspersky Security Network jest włączone](#), Kaspersky Endpoint Security wysyła do KSN pytanie odnośnie reputacji aplikacji za każdym razem, gdy jest ona uruchamiana. W oparciu o uzyskaną odpowiedź, aplikacja może zostać przeniesiona do grupy zaufania, która jest inna niż ta określona w ustawienia komponentu Ochrona przed włamaniami.
6. Użyj pola **Aktualizuj uprawnienia dla wcześniej nieznanymi aplikacji z bazy danych KSN**, aby skonfigurować automatyczną aktualizację uprawnień nieznanymi aplikacji.
7. Zapisz swoje zmiany.

[Jak wybrać grupę zaufania dla nieznanymi aplikacji w interfejsie aplikacji?](#)

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. W sekcji **Reguły działania aplikacji** wybierz odpowiednią grupę zaufania.
Jeśli uczestnictwo w [Kaspersky Security Network jest włączone](#), Kaspersky Endpoint Security wysyła do KSN pytanie odnośnie reputacji aplikacji za każdym razem, gdy jest ona uruchamiana. W oparciu o uzyskaną odpowiedź, aplikacja może zostać przeniesiona do grupy zaufania, która jest inna niż ta określona w ustawienia komponentu Ochrona przed włamaniami.
4. Użyj pola **Uaktualnij reguły dla wcześniej nieznanymi aplikacji z KSN**, aby skonfigurować automatyczną aktualizację uprawnień nieznanymi aplikacji.
5. Zapisz swoje zmiany.

Wybieranie grupy zaufania dla cyfrowo podpisanych aplikacji

Kaspersky Endpoint Security zawsze umieszcza aplikacje podpisane certyfikatami firmy Microsoft lub certyfikatami firmy Kaspersky w grupie Zaufane.


[Jak wybrać grupę zaufania dla cyfrowo podpisanych aplikacji w Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
6. W sekcji **Reguły działania aplikacji** użyj pola **Ufaj aplikacjom podpisanym cyfrowo**, aby włączyć lub wyłączyć automatyczne przypisywanie do grupy Zaufane dla aplikacji zawierających podpis cyfrowy zaufanych producentów.
Zaufani producenci to producenci oprogramowania, którzy zostali umieszczeni w grupie zaufania przez Kaspersky. Możesz także ręcznie [dodać certyfikat producenta do zaufanych certyfikatów systemowych](#).
Jeśli pole nie jest zaznaczone, Ochrona przed włamaniami nie uważa aplikacji posiadających podpis cyfrowy za zaufane i wykorzystuje inne parametry do określenia ich [grupy zaufania](#).
7. Zapisz swoje zmiany.

[Jak wybrać grupę zaufania dla cyfrowo podpisanych aplikacji w Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
5. W sekcji **Reguły działania aplikacji** użyj pola **Ufaj aplikacjom podpisanym cyfrowo**, aby włączyć lub wyłączyć automatyczne przypisywanie do grupy Zaufane dla aplikacji zawierających podpis cyfrowy zaufanych producentów.
Zaufani producenci to producenci oprogramowania, którzy zostali umieszczeni w grupie zaufania przez Kaspersky. Możesz także ręcznie [dodać certyfikat producenta do zaufanych certyfikatów systemowych](#).
Jeśli pole nie jest zaznaczone, Ochrona przed włamaniami nie uważa aplikacji posiadających podpis cyfrowy za zaufane i wykorzystuje inne parametry do określenia ich [grupy zaufania](#).
6. Zapisz swoje zmiany.

[Jak wybrać grupę zaufania dla cyfrowo podpisanych aplikacji w interfejsie aplikacji?](#)

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. W sekcji **Reguły działania aplikacji** użyj pola **Ufaj aplikacjom podpisanym cyfrowo**, aby włączyć lub wyłączyć automatyczne przypisywanie do grupy Zaufane dla aplikacji zawierających podpis cyfrowy zaufanych producentów.

Zaufani producenci to producenci oprogramowania, którzy zostali umieszczeni w grupie zaufania przez Kaspersky. Możesz także ręcznie [dodać certyfikat producenta do zaufanych certyfikatów systemowych](#).

Jeśli pole nie jest zaznaczone, Ochrona przed włamaniami nie uważa aplikacji posiadających podpis cyfrowy za zaufane i wykorzystuje inne parametry do określenia ich [grupy zaufania](#).

4. Zapisz swoje zmiany.

Zarządzanie uprawnieniami aplikacji

Domyślnie, aktywność aplikacji jest kontrolowana w oparciu o uprawnienia aplikacji, które są definiowane dla określonej [grupy zaufania](#), do której Kaspersky Endpoint Security przypisał aplikację przy jej pierwszym uruchomieniu. Jeżeli jest to konieczne, możesz [zmodyfikować uprawnienia aplikacji dla całej grupy zaufania](#), dla pojedynczej aplikacji lub grupy aplikacji znajdujących się w grupie zaufania.

Ręcznie zdefiniowane uprawnienia aplikacji posiadają wyższy priorytet niż uprawnienia aplikacji, które zostały zdefiniowane dla grupy zaufania. Innymi słowy, jeśli ręcznie zdefiniowane uprawnienia aplikacji różnią się od uprawnień aplikacji zdefiniowanych dla grup zaufania, komponent Ochrona przed włamaniami kontroluje aktywność aplikacji zgodnie z ręcznie zdefiniowanymi uprawnieniami aplikacji.

Reguły, które tworzysz dla aplikacji, są dziedziczone przez aplikacje potomne. Na przykład, jeśli zablokujesz całą aktywność sieciową dla cmd.exe, cała aktywność sieciowa zostanie także zablokowana dla notepad.exe, gdy zostanie uruchomiony przy użyciu cmd.exe. Jeśli aplikacja jest uruchamiana niebezpośrednio przez inną aplikację, ale nie jest potomną aplikacją, z której jest uruchamiana, reguły nie są dziedziczone.

[Jak zmienić uprawnienia aplikacji w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
 2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
 3. W obszarze roboczym wybierz zakładkę **Profile**.
 4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
 5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
 6. W sekcji **Reguły kontroli aplikacji oraz chronionych zasobów** kliknij **Ustawienia**.
To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
 7. Wybierz zakładkę **Uprawnienia aplikacji**.
 8. Kliknij przycisk **Dodaj**.
 9. W otwartym oknie wprowadź kryteria wyszukiwania aplikacji, której uprawnienia chcesz zmienić.
Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki ***** i **?**.
 10. Kliknij przycisk **Odśwież**.
Kaspersky Endpoint Security wyszuka aplikację na skonsolidowanej liście aplikacji zainstalowanych na zarządzanych komputerach. Kaspersky Endpoint Security wyświetli listę aplikacji spełniających Twoje kryteria wyszukiwania.
 11. Wybierz żadaną aplikację.
 12. Z listy rozwijalnej **Dodaj wybraną aplikację do grupy zaufania** wybierz **Domyślne grupy** i kliknij **OK**.
Aplikacja zostanie dodana do domyślnej grupy.
 13. Wybierz odpowiednią aplikację, a następnie wybierz **Uprawnienia aplikacji** z menu kontekstowego aplikacji.
Spowoduje to otwarcie właściwości aplikacji.
 14. Wykonaj jedną z poniższych czynności:
 - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz zakładkę **Pliki i rejestr systemu**.
 - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz zakładkę **Uprawnienia**.
- Aktywność sieciowa aplikacji jest kontrolowana przez [Zapora sieciową](#) za pomocą *reguł sieciowych*.
15. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania kliknij je prawym klawiszem myszy, aby otworzyć menu kontekstowe i wybrać odpowiednią opcję: **Dziedzicz** (✓) lub **Zablokuj** (⊘).
 16. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** (✓ / ⊘).

Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.

17. Zapisz swoje zmiany.

[Jak zmienić uprawnienia aplikacji w Web Console i Cloud Console?](#) 





1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
5. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij odnośnik **Uprawnienia aplikacji i zasoby chronione**.
To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
6. Wybierz zakładkę **Uprawnienia aplikacji**.
W lewej części okna zobaczysz listę grup zaufania, a w prawej części okna zobaczysz i ich właściwości.
7. Kliknij przycisk **Dodaj**.
To spowoduje uruchomienie Kreatora dodawania aplikacji do grupy zaufania.
8. Wybierz odpowiednią grupę zaufania dla aplikacji.
9. Wybierz typ **Aplikacja**. Kliknij przycisk **Dalej**.
Jeśli chcesz zmienić grupę zaufania dla kilku aplikacji, wybierz typ **Grupa** i określ nazwę grupy zaufania.
10. Z otwartej listy aplikacji wybierz aplikację, dla których chcesz zmienić uprawnienia aplikacji.
Użyj filtra. Możesz wprowadzić nazwę aplikacji lub nazwę producenta. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki * i ?.
11. Zakończ działanie kreatora, klikając **OK**.
Aplikacja zostanie dodana do grupy zaufania.
12. W lewej części okna wybierz odpowiednią aplikację.
13. W prawej części okna, z listy rozwijalnej wykonaj jedną z następujących czynności:
 - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz **Pliki i rejestr systemu**.
 - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz **Uprawnienia**.

Aktywność sieciowa aplikacji jest kontrolowana przez [Zaporę sieciową](#) za pomocą *reguł sieciowych*.

14. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania wybierz odpowiednią opcję: **Dziedzicz**, **Zezwól** (✔) lub **Zablokuj** (✘).
15. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** (✔ / ✘).
Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacjach, które używają każdego zasobu.

16. Zapisz swoje zmiany.

[Jak zmienić uprawnienia aplikacji w interfejsie aplikacji?](#) 

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. Kliknij przycisk **Zarządzaj aplikacjami**.
Spowoduje to otwarcie listy zainstalowanych aplikacji.
4. Wybierz żadaną aplikację.
5. Z menu kontekstowego aplikacji wybierz **Szczegóły i reguły**.
Spowoduje to otwarcie właściwości aplikacji.
6. Wykonaj jedną z poniższych czynności:
 - Jeśli chcesz zmodyfikować uprawnienia aplikacji zarządzające wykonywaniem operacji na rejestrze systemu operacyjnego, plikach użytkowników i ustawieniach aplikacji, wybierz zakładkę **Pliki i rejestr systemu**.
 - Jeśli chcesz zmodyfikować uprawnienia grupy zaufania, które zarządzają dostępem do obiektów i procesów systemu operacyjnego, wybierz zakładkę **Uprawnienia**.
7. Dla odpowiedniego zasobu, w kolumnie odpowiedniego działania kliknij je prawym klawiszem myszy, aby otworzyć menu kontekstowe i wybrać odpowiednią opcję: **Dziedzicz**, **Zezwól**  lub **Zablokuj** .
8. Jeśli chcesz monitorować korzystanie z zasobów komputera, wybierz **Zapisuj zdarzenia** .
Kaspersky Endpoint Security zapisze informacje o działaniu komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.
9. Wybierz zakładkę **Wykluczenia** i skonfiguruj zaawansowane ustawienia aplikacji (patrz tabela poniżej).
10. Zapisz swoje zmiany.

Zaawansowane ustawienia aplikacji

Parametr	Opis
Nie skanuj otwieranych plików	Wszystkie pliki, które są otwierane przez aplikację, zostają wykluczone ze skanowania wykonywanego przez program Kaspersky Endpoint Security. Na przykład, jeśli używasz aplikacji do tworzenia kopii zapasowej plików, ta funkcja pomaga w zmniejszeniu zużycia zasobów przez Kaspersky Endpoint Security.
Nie monitoruj aktywności aplikacji	Kaspersky Endpoint Security nie będzie monitorował aktywności sieciowej i plikowej aplikacji w systemie operacyjnym. Aktywność aplikacji jest monitorowana przez następujące komponenty: Wykrywanie zachowań , Ochrona przed exploitami , Ochrona przed włamaniami , Silnik korygujący i Zapora sieciowa .
Nie dziedzicz ograniczeń nadrzędnego procesu (aplikacji)	Ograniczenia skonfigurowane dla procesu nadrzędnego nie będą stosowane przez program Kaspersky Endpoint Security do procesu podrzędnego. Proces nadrzędny jest uruchamiany przez aplikację, dla której skonfigurowano uprawnienia aplikacji (Ochrona przed włamaniami) i reguły sieciowe dla aplikacji (Zapora sieciowa).
Nie monitoruj aktywności aplikacji potomnych	Kaspersky Endpoint Security nie będzie monitorował aktywności plikowej i sieciowej aplikacji, które są uruchamiane przez tę aplikację.

Zezwól na interakcję z interfejsem aplikacji	Autoochrona Kaspersky Endpoint Security blokuje wszystkie próby zarządzania usługami aplikacji ze zdalnego komputera. Jeśli pole jest zaznaczone, aplikacja do zdalnej administracji może zarządzać ustawieniami Kaspersky Endpoint Security poprzez interfejs Kaspersky Endpoint Security.
Nie skanuj szyfrowanego ruchu sieciowego / Nie skanuj całego ruchu sieciowego	Ruch sieciowy zainicjowany przez aplikację zostanie wykluczony ze skanowania wykonywanego przez Kaspersky Endpoint Security. Ze skanowania można wykluczyć cały ruch sieciowy lub tylko zaszyfrowany ruch sieciowy. Ze skanowania możesz także wykluczyć pojedyncze adresy IP i numery portów.

Ochrona zasobów systemu operacyjnego i danych osobowych

Komponent Ochrona przed włamaniami zarządza uprawnieniami aplikacji do podejmowania działań na różnych kategoriach zasobów systemu operacyjnego i danych osobistych. Specjaliści z Kaspersky utworzyli listę predefiniowanych kategorii chronionych zasobów. Na przykład, kategoria *System operacyjny* zawiera podkategorię *Ustawienia uruchamiania*, która wyświetla wszystkie klucze rejestru skojarzone z automatycznym uruchamianiem aplikacji. Nie możesz zmieniać ani usuwać predefiniowanych kategorii chronionych zasobów ani chronionych zasobów znajdujących się w tych kategoriach.



[Jak dodawać chronione zasoby w Konsoli administracyjnej.\(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
6. W sekcji **Reguły kontroli aplikacji oraz chronionych zasobów** kliknij **Ustawienia**.
To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
7. Wybierz zakładkę **Chronione zasoby**.
W lewej części okna zostanie wyświetlona lista chronionych zasobów oraz odpowiednie uprawnienia dostępu do tych zasobów w zależności od określonej grupy zaufania.
8. Wybierz kategorię chronionych zasobów, do których chcesz dodać nowy chroniony zasób.
Jeśli chcesz dodać podkategorię, kliknij **Dodaj** → **Kategoria**.
9. Kliknij przycisk **Dodaj**. Z listy rozwijalnej wybierz typ zasobu, który chcesz dodać: **Plik lub folder** lub **Klucz rejestru**.
10. W otwartym oknie wybierz plik, folder lub klucz rejestru.
Możesz przejrzeć uprawnienia aplikacji do uzyskania dostępu do dodanych zasobów. Aby to zrobić, w lewej części okna wybierz dodany zasób, a Kaspersky Endpoint Security wyświetli uprawnienia dostępu dla każdej grupy zaufania. Możesz także wyłączyć kontrolę aktywności aplikacji na zasobach, używając pola obok nowego zasobu.
11. Zapisz swoje zmiany.

[Jak dodać chroniony zasób w Web Console i Cloud Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
5. W sekcji **Uprawnienia aplikacji i zasoby chronione** kliknij odnośnik **Uprawnienia aplikacji i zasoby chronione**.
To spowoduje otwarcie okna konfiguracji uprawnień aplikacji oraz listy chronionych zasobów.
6. Wybierz zakładkę **Chronione zasoby**.
W lewej części okna zostanie wyświetlona lista chronionych zasobów oraz odpowiednie uprawnienia dostępu do tych zasobów w zależności od określonej grupy zaufania.
7. Kliknij przycisk **Dodaj**.
Zostanie uruchomiony Kreator tworzenia nowego zasobu.
8. Kliknij odnośnik **Nazwa grupy**, aby wybrać kategorię chronionych zasobów, do których chcesz dodać nowy chroniony zasób.
Jeśli chcesz dodać podkategorię, wybierz opcję **Kategoria chronionych zasobów**.
9. Wybierz typ zasobu, który chcesz dodać: **Plik lub folder** lub **Klucz rejestru**.
10. Wybierz plik, folder lub klucz rejestru.
11. Zakończ działanie kreatora, klikając **OK**.
Możesz przejrzeć uprawnienia aplikacji do uzyskania dostępu do dodanych zasobów. Aby to zrobić, w lewej części okna wybierz dodany zasób, a Kaspersky Endpoint Security wyświetli uprawnienia dostępu dla każdej grupy zaufania. Możesz także użyć pola w kolumnie **Stan**, aby wyłączyć kontrolę aktywności aplikacji na zasobach.
12. Zapisz swoje zmiany.

[Jak dodać chroniony zasób w interfejsie aplikacji?](#) 

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. Kliknij przycisk **Zarządzaj zasobami**.
Zostanie otwarta lista chronionych zasobów.
4. Wybierz kategorię chronionych zasobów, do których chcesz dodać nowy chroniony zasób.
Jeśli chcesz dodać podkategorię, kliknij **Dodaj** → **Kategoria**.
5. Kliknij przycisk **Dodaj**. Z listy rozwijalnej wybierz typ zasobu, który chcesz dodać: **Plik lub folder** lub **Klucz rejestru**.
6. W otwartym oknie wybierz plik, folder lub klucz rejestru.
Możesz przejrzeć uprawnienia aplikacji do uzyskania dostępu do dodanych zasobów. Aby to zrobić, w lewej części okna wybierz dodany zasób, a Kaspersky Endpoint Security wyświetli listę aplikacji i uprawnienia dostępu dla każdej aplikacji. Możesz wyłączyć kontrolę aktywności aplikacji na zasobach, używając przycisku  **Wyłącz kontrolę** w kolumnie **Stan**.
7. Zapisz swoje zmiany.

Kaspersky Endpoint Security będzie kontrolował dostęp do dodanych zasobów systemu operacyjnego i do danych osobowych. Kaspersky Endpoint Security kontroluje dostęp aplikacji do zasobów w oparciu o grupę zaufania przypisaną do aplikacji. Możesz także [zmienić grupę zaufania aplikacji](#).

Usuwanie informacji o nieużywanych aplikacjach

Kaspersky Endpoint Security używa uprawnień aplikacji do kontrolowania aktywności aplikacji. Uprawnienia aplikacji są określone przez ich grupę zaufania. Kaspersky Endpoint Security umieszcza aplikację w [grupie zaufania](#), gdy aplikacja jest uruchamiana po raz pierwszy. Możesz [ręcznie zmienić grupę zaufania aplikacji](#). Możesz także [ręcznie skonfigurować uprawnienia poszczególnych aplikacji](#). Kaspersky Endpoint Security przechowuje następujące informacje o aplikacji: grupę zaufania aplikacji i uprawnienia aplikacji.

Kaspersky Endpoint Security automatycznie usuwa informacje o nieużywanych aplikacjach, aby zaoszczędzić zasoby komputera. Kaspersky Endpoint Security usuwa informacje o aplikacji zgodnie z następującymi regułami:

- Jeśli grupa zaufania i uprawnienia aplikacji zostały określone automatycznie, Kaspersky Endpoint Security usunie informacje o tej aplikacji po 30 dniach. Nie jest możliwa zmiana okresu przechowywania informacji o aplikacji ani wyłączenie automatycznego usuwania.
- Jeśli ręcznie umieścisz aplikację w grupie zaufania lub skonfigurujesz jej uprawnienia dostępu, Kaspersky Endpoint Security usunie informacje o tej aplikacji po 60 dniach (domyślny okres przechowywania). Możesz zmienić okres przechowywania informacji o aplikacji lub wyłączyć automatyczne usuwanie (patrz instrukcje poniżej).

Po uruchomieniu aplikacji, której informacje zostały usunięte, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

[Jak skonfigurować automatyczne usuwanie informacji o nieużywanych aplikacjach w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
6. W sekcji **Reguły działania aplikacji** wykonaj jedną z poniższych czynności:
 - Jeśli chcesz skonfigurować automatyczne usuwanie, zaznacz pole wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni** i wprowadź liczbę dni.


Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu zostaną usunięte przez Kaspersky Endpoint Security po upływie określonej liczbie dni. Informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone, zostaną również usunięte przez Kaspersky Endpoint Security po 30 dniach.
 - Jeśli chcesz wyłączyć automatyczne usuwanie, odznacz pole wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni**.

Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu będą przechowywane przez Kaspersky Endpoint Security na czas nieokreślony, bez żadnych ograniczeń czasu przechowywania. Kaspersky Endpoint Security usunie tylko informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone po 30 dniach.
7. Zapisz swoje zmiany.

[Jak skonfigurować automatyczne usuwanie informacji o nieużywanych aplikacjach w Web Console i Cloud Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
5. W sekcji **Reguły działania aplikacji** wykonaj jedną z poniższych czynności:
 - Jeśli chcesz skonfigurować automatyczne usuwanie, zaznacz pole wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni** i wprowadź liczbę dni.
Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu zostaną usunięte przez Kaspersky Endpoint Security po upływie określonej liczbie dni. Informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone, zostaną również usunięte przez Kaspersky Endpoint Security po 30 dniach.
 - Jeśli chcesz wyłączyć automatyczne usuwanie, odznacz pole wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni**.
Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu będą przechowywane przez Kaspersky Endpoint Security na czas nieokreślony, bez żadnych ograniczeń czasu przechowywania. Kaspersky Endpoint Security usunie tylko informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone po 30 dniach.
6. Zapisz swoje zmiany.

[Jak skonfigurować automatyczne usuwanie informacji o nieużywanych aplikacjach w interfejsie aplikacji?](#)

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Ochrona przed włamaniami**.
3. W sekcji **Reguły działania aplikacji** wykonaj jedną z poniższych czynności:
 - Jeśli chcesz skonfigurować automatyczne usuwanie, zaznacz pole wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni** i wprowadź liczbę dni.
Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu zostaną usunięte przez Kaspersky Endpoint Security po upływie określonej liczbie dni. Informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone, zostaną również usunięte przez Kaspersky Endpoint Security po 30 dniach.
 - Jeśli chcesz wyłączyć automatyczne usuwanie, odznacz pole wyboru **Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni**.
Informacje o aplikacjach, które ręcznie umieścisz w grupie zaufania lub których ręcznie skonfigurowane uprawnienia dostępu będą przechowywane przez Kaspersky Endpoint Security na czas nieokreślony, bez żadnych ograniczeń czasu przechowywania. Kaspersky Endpoint Security usunie tylko informacje o aplikacjach, których grupa zaufania i uprawnienia aplikacji zostały automatycznie określone po 30 dniach.
4. Zapisz swoje zmiany.

Monitorowanie Ochrony przed włamaniami

Możesz otrzymać raporty z działania komponentu Ochrona przed włamaniami. Raporty zawierają informacje o działaniach na zasobach komputera wykonywanych przez aplikację (dozwolone lub zabronione). Raporty także zawierają informacje o aplikacji, które używają każdego zasobu.

Aby monitorować działania komponentu Ochrona przed włamaniami, musisz włączyć zapisywanie do raportu. Na przykład, możesz [włączyć przekazywanie raportów dla pojedynczych aplikacji w ustawieniach komponentu Ochrona przed włamaniami](#).

Podczas konfigurowania monitorowania Ochrony przed włamaniami należy wziąć pod uwagę potencjalne obciążenie sieci, gdy przekazywane są zdarzenia do Kaspersky Security Center. Możesz też włączyć zapisywanie raportów tylko w dzienniku lokalnym programu Kaspersky Endpoint Security.

Ochrona dostępu do audio i wideo

Cyberprzestępcy mogą używać specjalnych programów w celu podjęcia próby uzyskania dostępu do urządzeń, które nagrywają audio i wideo (takich jak mikrofony lub kamery internetowe). Kaspersky Endpoint Security kontroluje, kiedy aplikacje uzyskują dostęp do strumienia audio i do strumienia wideo oraz chronią dane przed nieautoryzowanym przechwytywaniem.

Domyślnie, Kaspersky Endpoint Security kontroluje dostęp aplikacji do strumienia audio i wideo w następujący sposób:

- Aplikacje należące do grupy Zaufane i Niski poziom ograniczeń mogą domyślnie uzyskiwać dostęp do strumienia audio i strumienia wideo z poziomu urządzeń.
- Aplikacje należące do grupy Wysoki poziom ograniczeń i Niezaufane mogą domyślnie uzyskiwać dostęp do strumienia audio i strumienia wideo z poziomu urządzeń.

Możesz [ręcznie zezwolić aplikacjom na uzyskiwanie dostępu do strumienia audio i strumienia wideo](#).

Specjalne funkcje ochrony strumienia audio

W przypadku ochrony strumienia audio należy mieć na uwadze następujące kwestie:

- Aby ta funkcjonalność mogła działać, [należy włączyć moduł Ochrona przed włamaniami](#).
- Jeśli aplikacja zaczęła odbierać strumień audio przed uruchomieniem Ochrony przed włamaniami, Kaspersky Endpoint Security zezwoli aplikacji na odbieranie strumienia audio i nie wyświetli żadnego komunikatu.
- Jeśli po rozpoczęciu odbierania przez aplikację strumienia audio przeniosłeś ją do grupy Niezaufane lub Wysoki poziom ograniczeń, Kaspersky Endpoint Security zezwoli aplikacji na odbieranie strumienia audio i nie wyświetli żadnego komunikatu.
- Po zmianie ustawień dostępu aplikacji do urządzeń rejestrujących dźwięk (na przykład, [jeśli dla aplikacji zablokowano możliwość odbierania strumienia audio](#)), ta aplikacja musi zostać uruchomiona ponownie, aby zatrzymać dla niej odbieranie strumienia audio.

- Kontrola dostępu urządzeń rejestrujących dźwięk do strumienia audio nie zależy od ustawień dostępu aplikacji do kamery internetowej.
- Kaspersky Endpoint Security chroni dostęp tylko do wbudowanych i zewnętrznych mikrofonów. Inne urządzenia rejestrujące dźwięk nie są obsługiwane.
- Kaspersky Endpoint Security nie może zagwarantować ochrony strumienia audio pochodzącego z takich urządzeń, jak aparaty DSLR (lustrzanki), kamery wideo oraz kamery sportowe.
- Jeśli uruchamiasz aplikacje rejestrujące dźwięk i obraz lub aplikacje do odtwarzania dźwięku i obrazu pierwszy raz od momentu zainstalowania Kaspersky Endpoint Security, działanie tych aplikacji może zostać przerwane. Jest to konieczne do włączenia funkcji kontrolującej dostęp aplikacji do urządzeń rejestrujących dźwięk. Usługi systemu kontrolujące sprzęt audio zostają uruchomione ponownie, gdy Kaspersky Endpoint Security jest uruchamiany po raz pierwszy.

Specjalne funkcje ochrony dostępu do kamery internetowej

Funkcja ochrony dostępu do kamery internetowej posiada następujące cechy i ograniczenia:

- Aplikacja kontroluje obraz wideo i nieruchome obrazy pochodzące z przetworzenia danych kamery internetowej.
- Aplikacja kontroluje strumień audio, jeśli jest on częścią strumienia wideo otrzymanego z kamery internetowej.
- Aplikacja kontroluje jedynie kamery podłączone do portów USB lub IEEE1394, które są wyświetlane w Menedżerze urządzeń systemu Windows jako **Urządzenia do obrazowania**.
- Kaspersky Endpoint Security obsługuje następujące kamery internetowe:
 - Logitech HD Webcam C270
 - Logitech HD Webcam C310
 - Logitech Webcam C210
 - Logitech Webcam Pro 9000
 - Logitech HD Webcam C525
 - Microsoft LifeCam VX-1000
 - Microsoft LifeCam VX-2000
 - Microsoft LifeCam VX-3000
 - Microsoft LifeCam VX-800
 - Microsoft LifeCam Cinema

Kaspersky nie gwarantuje obsługi kamer internetowych, które nie znajdują się na tej liście.

Silnik korygujący

Silnik korygujący umożliwia Kaspersky Endpoint Security wycofanie działań, które zostały wykonane przez szkodliwe oprogramowanie w systemie operacyjnym.

Podczas cofania szkodliwej aktywności w systemie operacyjnym Kaspersky Endpoint Security podejmuje działanie na następujących typach szkodliwej aktywności:

- **Aktywność plikowa**

Kaspersky Endpoint Security wykonuje następujące działania:

- Usuwa pliki wykonywalne, które zostały utworzone przez szkodliwe oprogramowanie (na wszystkich mediach za wyjątkiem dysków sieciowych).
- Usuwa pliki wykonywalne, które zostały utworzone przez programy, do których przeniknęło szkodliwe oprogramowanie.
- Przywraca pliki, które zostały zmodyfikowane lub usunięte przez szkodliwe oprogramowanie.

Funkcja odzyskiwania plików posiada [kilka ograniczeń](#).

- **Aktywność w rejestrze**

Kaspersky Endpoint Security wykonuje następujące działania:

- Usuwa klucze rejestru, które zostały utworzone przez szkodliwe oprogramowanie.
- Nie przywraca kluczy rejestru, które zostały zmodyfikowane lub usunięte przez szkodliwe oprogramowanie.

- **Aktywność w systemie**

Kaspersky Endpoint Security wykonuje następujące działania:

- Kończy procesy, które zostały zainicjowane przez szkodliwe oprogramowanie.
- Kończy procesy, do których przeniknęła szkodliwa aplikacja.
- Nie wznawia procesów zatrzymanych przez szkodliwy program.

- **Aktywność sieciowa**

Kaspersky Endpoint Security wykonuje następujące działania:

- Blokuję aktywność sieciową szkodliwego oprogramowania.
- Blokuję aktywność sieciową procesów, do których przeniknęło szkodliwe oprogramowanie.

Wycofanie działań szkodliwych programów może być zainicjowane przez komponent [Ochrona plików](#) lub [Wykrywanie zachowań](#) lub podczas [skanowania antywirusowego](#).

Wycofywanie działań szkodliwego oprogramowania oddziałuje na ściśle określony zestaw danych. Nie ma negatywnego wpływu na system operacyjny i integralność danych komputera.


[Jak włączyć lub wyłączyć komponent Silnik korygujący w Konsoli administracyjnej.\(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Zaawansowana ochrona przed zagrożeniami** → **Silnik korygujący**.
6. Użyj pola **Silnik korygujący**, aby włączyć lub wyłączyć komponent.
7. Zapisz swoje zmiany.

[Jak włączyć lub wyłączyć komponent Silnik korygujący w Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Zaawansowana ochrona przed zagrożeniami** → **Silnik korygujący**.
5. Użyj przełącznika **Silnik korygujący**, aby włączyć lub wyłączyć komponent.
6. Zapisz swoje zmiany.

[Jak włączyć lub wyłączyć komponent Silnik korygujący w interfejsie aplikacji?](#)

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Silnik korygujący**.
3. Użyj przełącznika **Silnik korygujący**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

W wyniku tego działania, jeśli Silnik korygujący jest włączony, Kaspersky Endpoint Security wycofa działania wykonane przez szkodliwe aplikacje w systemie operacyjnym.

Kaspersky Security Network

Aby lepiej chronić Twój komputer, Kaspersky Endpoint Security wykorzystuje dane otrzymane od użytkowników z całego świata. Usługa Kaspersky Security Network została zaprojektowana do gromadzenia tych danych.

Kaspersky Security Network (KSN) jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Endpoint Security na nowe zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. Jeśli uczestniczysz w Kaspersky Security Network, usługi KSN zapewniają Kaspersky Endpoint Security informacje o kategorii i reputacji przeskanowanych plików, a także informacje o reputacji przeskanowanych adresów internetowych.

Korzystanie z Kaspersky Security Network jest dobrowolne. Aplikacja oferuje użytkownikowi możliwość korzystania z KSN podczas wstępnej konfiguracji aplikacji. Użytkownik może rozpocząć lub zakończyć uczestniczenie w KSN w dowolnym momencie.

Więcej informacji na temat wysyłania do Kaspersky informacji statystycznych, wygenerowanych w trakcie uczestnictwa w KSN, a także informacji o przechowywaniu i niszczeniu takich informacji można znaleźć w Umowie Kaspersky Security Network oraz na [stronie Kaspersky](#). Plik ksn_<ID języka>.txt zawierający treść Oświadczenia Kaspersky Security Network znajduje się w [pakiecie dystrybucyjnym](#) aplikacji.

Aby zmniejszyć obciążenie na serwerach KSN, eksperci z Kaspersky mogą opublikować aktualizacje aplikacji, które tymczasowo wyłączą lub częściowo ograniczą żądania do Kaspersky Security Network. W tym przypadku stan połączenia z KSN w lokalnym interfejsie aplikacji jest *Włączony z ograniczeniami*.

Infrastruktura KSN

Kaspersky Endpoint Security obsługuje następujące rozwiązania infrastrukturalne KSN:

- *Globalna sieć KSN* to rozwiązanie używane przez większość aplikacji Kaspersky. Uczestnicy KSN otrzymują informacje z Kaspersky Security Network i wysyłają do Kaspersky informacje o obiektach wykrytych na komputerze użytkownika w celu dodatkowego przeanalizowania przez analityków Kaspersky i znajdujących się w bazach danych reputacji oraz statystycznych bazach danych usługi Kaspersky Security Network.
- *Prywatna sieć KSN* to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów. Prywatna sieć KSN została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z dowolnego z następujących powodów:
 - Lokalne stacje robocze nie są połączone z internetem.
 - Przesyłanie wszelkich danych poza kraj lub poza korporacyjną sieć LAN są zabronione przez prawo lub ograniczone przez politykę bezpieczeństwa firmy.

Domyślnie Kaspersky Security Center używa Global KSN. Możesz skonfigurować użycie Prywatnej sieci KSN w Konsoli administracyjnej (MMC) i Kaspersky Security Center Web Console oraz w [wierszu polecenia](#). Nie można skonfigurować korzystania z Prywatnej sieci KSN w konsoli Kaspersky Security Center Cloud Console.

Więcej informacji o Prywatnej sieci KSN można znaleźć w *dokumentacji do Kaspersky Private Security Network*.

KSN Proxy

Komputery użytkowników zarządzane przez Kaspersky Security Center Administration Server mogą komunikować się z KSN poprzez usługę KSN Proxy.

Usługa KSN Proxy posiada następujące możliwości:

- Komputer użytkownika może łatwo odpytywać KSN i przysyłać informacje do KSN, nawet bez bezpośredniego dostępu do internetu.
- Usługa KSN Proxy buforuje przetwarzane dane, ograniczając obciążenie zewnętrznego kanału komunikacji sieciowej i przyspieszając odbieranie informacji żądanych przez komputer użytkownika.

Więcej informacji na temat usługi KSN Proxy można znaleźć w [pomocy do Kaspersky Security Center](#).

Włączanie i wyłączanie korzystania z Kaspersky Security Network

W celu włączenia lub wyłączenia korzystania z Kaspersky Security Network:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Kaspersky Security Network**.
3. Użyj przełącznika **Kaspersky Security Network**, aby włączyć lub wyłączyć komponent.
Jeśli włączyć korzystanie z KSN, Kaspersky Endpoint Security wyświetli Oświadczenie Kaspersky Security Network. Przeczytaj i zaakceptuj (jeśli wyrażasz na nie zgodę) warunki korzystania Oświadczenia Kaspersky Security Network (KSN).
Domyślnie, Kaspersky Endpoint Security używa Rozszerzonego trybu KSN. *Rozszerzony tryb KSN* to tryb, w którym Kaspersky Endpoint Security wysyła [dodatkowe dane](#) do Kaspersky.
4. Jeśli to konieczne, przesunij przełącznik **Włącz rozszerzony tryb KSN** na pozycję wyłączenia.
5. Zapisz swoje zmiany.

W wyniku tego działania, jeśli korzystanie z KSN jest włączone, Kaspersky Endpoint Security używa informacji o reputacji plików, zasobów sieciowych i aplikacji, otrzymanych z Kaspersky Security Network.

Ograniczenia Private KSN

Private KSN (zwana dalej również KPSN) umożliwia korzystanie z własnych lokalnych baz danych reputacji do sprawdzania reputacji obiektów (pliki lub adresy internetowe). Reputacja obiektu dodanego do lokalnej bazy danych reputacji posiada wyższy priorytet niż obiektu dodanego do KSN/KPSN. Na przykład, Kaspersky Endpoint Security skanuje komputer i żąda reputacji pliku z KSN/KPSN. Jeśli plik posiada „niezaufaną” reputację w lokalnej bazie danych reputacji, ale posiada „zaufaną” reputację w KSN/KPSN, Kaspersky Endpoint Security wykryje plik jako „niezaufany” i podejmie działanie zdefiniowane dla wykrytych zagrożeń.

Jednakże w niektórych przypadkach Kaspersky Endpoint Security może nie zażądać reputacji obiektu z KSN/KPSN. W takiej sytuacji Kaspersky Endpoint Security nie otrzyma danych z lokalnej bazy danych reputacji KPSN. Kaspersky Endpoint Security może nie zażądać reputacji obiektu z KSN/KPSN z następujących względów:

- Aplikacje firmy Kaspersky wykorzystują bazy danych reputacji offline. Bazy danych reputacji offline zostały zaprojektowane do optymalizacji zasobów podczas działania firmy Kaspersky i do ochrony krytycznie ważnych obiektów na komputerze. Bazy danych reputacji offline są tworzone przez ekspertów z Kaspersky w oparciu o dane z Kaspersky Security Network. Aplikacje firmy Kaspersky aktualizują bazy danych reputacji offline wraz z antywirusowymi bazami danych określonej aplikacji. Jeśli bazy danych reputacji offline zawierają informacje o skanowanym obiekcie, aplikacja nie żąda reputacji tego obiektu z KSN/KPSN.


- Wykluczenia ze skanowania ([strefa zaufana](#)) są konfigurowane w ustawieniach aplikacji. W takim przypadku aplikacja nie weźmie pod uwagę reputacji obiektu w lokalnej bazie danych reputacji.
- Aplikacja wykorzystuje technologie optymalizacji skanowania, takie jak iSwift lub iChecker, lub buforuje żądania reputacji do KSN / KPSN. Jeśli taka sytuacja ma miejsce, aplikacja może nie zażądać reputacji wcześniej skanowanych obiektów.
- Aby zoptymalizować jego obciążenie, aplikacja skanuje pliki pewnego formatu i rozmiaru. Lista odpowiednich formatów i ograniczeń rozmiaru została określona przez ekspertów z Kaspersky. Ta lista jest aktualizowana o antywirusowe bazy danych aplikacji. Ustawienia optymalizacji skanowania możesz skonfigurować także w interfejsie aplikacji, na przykład, dla [komponentu Ochrona plików](#).

Włączanie i wyłączanie dla składników ochrony trybu chmury

Tryb chmury odnosi się do trybu działania aplikacji, w którym Kaspersky Endpoint Security używa lekkiej wersji antywirusowych baz danych. Kaspersky Security Network obsługuje działanie aplikacji, gdy używana jest lekka wersja antywirusowych baz danych. Lekka wersja antywirusowych baz danych umożliwia korzystanie z około połowy pamięci RAM komputera, która inaczej zostałaby użyta ze zwykłymi bazami danych. Jeśli nie uczestniczysz w Kaspersky Security Network lub jeśli tryb chmury jest wyłączony, Kaspersky Endpoint Security pobierze pełną wersję antywirusowych baz danych z serwerów Kaspersky.

Podczas korzystania z Kaspersky Private Security Network, funkcjonalność trybu chmury jest dostępna począwszy od Kaspersky Private Security Network w wersji 3.0.

W celu włączenia lub wyłączenia dla składników ochrony trybu chmury:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Zaawansowana ochrona przed zagrożeniami** → **Kaspersky Security Network**.
3. Użyj przełącznika **Włącz tryb chmury**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

W wyniku tego działania, Kaspersky Endpoint Security pobiera lżejszą wersję lub pełną wersję antywirusowych baz danych podczas kolejnej aktualizacji.

Jeśli podstawowa wersja antywirusowych baz danych nie jest dostępna do użycia, Kaspersky Endpoint Security automatycznie przełączy do wersji premium antywirusowych baz danych.

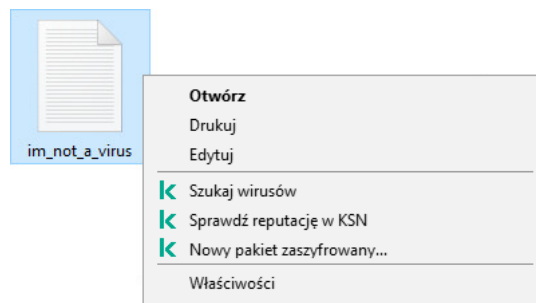
Sprawdzanie reputacji pliku w Kaspersky Security Network

Jeśli masz wątpliwości co do bezpieczeństwa pliku, możesz sprawdzić jego reputację w Kaspersky Security Network.

Możesz sprawdzić reputację pliku, jeśli zaakceptowałeś warunki [Oświadczenia Kaspersky Security Network](#).

W celu sprawdzenia reputacji pliku w Kaspersky Security Network:


Otwórz menu kontekstowe pliku i wybierz opcję **Sprawdź reputację w KSN** (patrz rysunek poniżej).




Menu kontekstowe pliku

Kaspersky Endpoint Security wyświetla reputację pliku:

 **Zaufana.** Większość użytkowników Kaspersky Security Network potwierdziło, że plik jest zaufany.

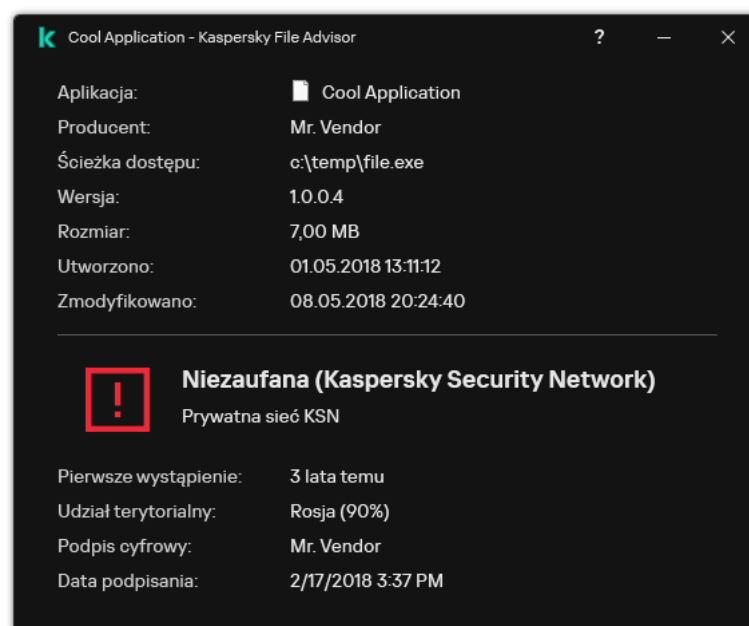
 **Legalne oprogramowanie, które może zostać wykorzystane przez intruzów do uszkodzenia komputera lub prywatnych danych.** Nie posiadają one żadnych szkodliwych funkcji, ale mogą zostać wykorzystane przez cyberprzestępców. Szczegółowe informacje o legalnym oprogramowaniu, które może zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych osobistych użytkownika, znajdują się na [stronie internetowej Encyklopedii IT Kaspersky](#). Możesz [dodać te aplikacje do listy zaufanych](#).

 **Niezaufane.** Wirus lub inna aplikacja, które [stwarzają zagrożenie](#).

 **Nieznane.** Kaspersky Security Network nie ma żadnych informacji o pliku. Możesz przeskanować plik przy użyciu antywirusowych baz danych (opcja **Szukaj wirusów** w menu kontekstowym).

Kaspersky Endpoint Security wyświetla rozwiązanie KSN, które zostało użyte do ustalenia reputacji pliku: *Globalna sieć KSN* lub *Prywatna sieć KSN*.

Kaspersky Endpoint Security wyświetla również dodatkowe informacje o pliku (patrz rysunek poniżej).



Skanowanie połączeń szyfrowanych

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.


Po instalacji Kaspersky Endpoint Security dodaje certyfikat Kaspersky do magazynu systemowego zaufanych certyfikatów (magazyn certyfikatów systemu Windows). Kaspersky Endpoint Security obejmuje również używanie magazynu systemowego zaufanych certyfikatów w Firefox i Thunderbird do skanowania ruchu sieciowego tych aplikacji.

Komponenty [Kontrola sieci](#), [Ochrona poczty](#), [Ochrona WWW](#) mogą deszyfrować i skanować ruch sieciowy przesyłany za pośrednictwem połączeń szyfrowanych przy użyciu następujących protokołów:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Konfigurowanie ustawień skanowania połączeń szyfrowanych

W celu skonfigurowania ustawień skanowania połączeń szyfrowanych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.
3. W sekcji **Skanowanie połączeń szyfrowanych** wybierz tryb skanowania połączeń szyfrowanych:
 - **Nie skanuj połączeń szyfrowanych** Kaspersky Endpoint Security nie będzie miał dostępu do zawartości stron internetowych, których adresy zaczynają się od `https://`.
 - **Skanuj połączenia szyfrowane po zgłoszeniach od składników ochrony**. Kaspersky Endpoint Security będzie skanował zaszyfrowany ruch sieciowy tylko na żądanie składników: Ochrona plików, Ochrona poczty i Ochrona WWW.
 - **Zawsze skanuj połączenia szyfrowane** Kaspersky Endpoint Security będzie skanował zaszyfrowany ruch sieciowy nawet wtedy, gdy składniki ochrony są wyłączone.

Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych, które zostały nawiązane przez [zaufane aplikacje, dla których skanowanie ruchu sieciowego jest wyłączone](#). Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych z predefiniowanej listy zaufanych stron internetowych. Predefiniowana lista zaufanych stron internetowych jest tworzona przez ekspertów Kaspersky. Ta lista jest aktualizowana o antywirusowe bazy danych aplikacji. Predefiniowaną listę zaufanych stron internetowych możesz przejrzeć tylko w interfejsie Kaspersky Endpoint Security. Listy nie można przejrzeć w Kaspersky Security Center Console.

4. W razie potrzeby [dodaj wyjątki skanowania: zaufane adresy i aplikacje](#).

5. Skonfiguruj ustawienia skanowania połączeń szyfrowanych (patrz tabela poniżej).

6. Zapisz swoje zmiany.

Ustawienia skanowania połączeń szyfrowanych

Parametr	Opis
Podczas odwiedzania domeny z niezaufanym certyfikatem	<ul style="list-style-type: none">• Zezwól. Jeśli ta opcja jest zaznaczona, podczas odwiedzania domeny z niezaufanym certyfikatem, Kaspersky Endpoint Security zezwoli na połączenie sieciowe. <p>Podczas otwierania domeny z niezaufanym certyfikatem w przeglądarce, Kaspersky Endpoint Security wyświetla stronę HTML pokazującą ostrzeżenie i powód, z jakiego odwiedzenie tej domeny nie jest zalecane. Użytkownik może kliknąć odnośnik ze strony ostrzegającej HTML, aby uzyskać dostęp do żądanego zasobu internetowego. Po kliknięciu tego odnośnika, w ciągu następnej godziny Kaspersky Endpoint Security nie wyświetli ostrzeżeń o niezaufanym certyfikacie podczas odwiedzania innych zasobów na tej samej domenie.</p> <ul style="list-style-type: none">• Blokuj połączenie. Jeśli ta opcja jest zaznaczona, podczas odwiedzania domeny z niezaufanym certyfikatem, Kaspersky Endpoint Security blokuje połączenie sieciowe. <p>Podczas otwierania domeny z niezaufanym certyfikatem w przeglądarce, Kaspersky Endpoint Security wyświetla stronę HTML pokazującą powód zablokowania tej domeny.</p>
W przypadku wystąpienia błędów skanowania połączenia szyfrowanego	<ul style="list-style-type: none">• Blokuj połączenie. Jeśli ten element jest wybrany, gdy wystąpi błąd skanowania połączenia szyfrowanego, Kaspersky Endpoint Security zablokuje połączenie sieciowe.• Dodaj domenę do wykluczeń. Jeśli ten element jest wybrany, gdy wystąpi błąd skanowania połączenia szyfrowanego, Kaspersky Endpoint Security doda domenę, w której wystąpił błąd, do listy domen z błędami skanowania i nie będzie monitorował szyfrowanego ruchu sieciowego, gdy ta domena będzie odwiedzana. Możesz przejrzeć listę domen z błędami skanowania połączeń szyfrowanych tylko w lokalnym interfejsie aplikacji. Aby wyczyścić zawartość listy, należy wybrać Zablokuj połączenie.
Zablokuj połączenia SSL 2.0 (zalecane)	<p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security zablokuje połączenia sieciowe nawiązane po protokole SSL 2.0.</p> <p>Jeśli pole jest odznaczone, Kaspersky Endpoint Security nie zablokuje połączeń sieciowych nawiązanych po protokole SSL 2.0 i nie będzie monitorował ruchu sieciowego przesyłanego przez te połączenia.</p>
Deszyfruj szyfrowane połączenia ze stronami internetowymi używającymi certyfikatów EV	<p>Certyfikaty EV (Extended Validation Certificates) potwierdzają autentyczność stron internetowych i zwiększają ochronę połączenia. Przeglądarki używają ikony kłódki w paskach adresu, aby pokazać, że strona internetowa posiada certyfikat EV. W przeglądarkach pasek adresu może być częściowo lub całkowicie oznaczony na zielono.</p> <p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security deszyfruje i monitoruje połączenia szyfrowane ze stronami internetowymi, które używają certyfikatu EV.</p>

Jeśli pole jest odznaczone, Kaspersky Endpoint Security nie ma dostępu do zawartości ruchu sieciowego HTTPS. Z tego powodu aplikacja monitoruje ruch sieciowy HTTPS tylko w oparciu o adres strony internetowej, na przykład: <https://google.com>.

Jeśli otwierasz stronę internetową z certyfikatem EV po raz pierwszy, zaszyfrowane połączenie zostanie odszyfrowane niezależnie od tego, czy pole jest zaznaczone.

Skanowanie połączeń szyfrowanych w Firefox i Thunderbird


Po instalacji Kaspersky Endpoint Security dodaje certyfikat Kaspersky do magazynu systemowego zaufanych certyfikatów (magazyn certyfikatów systemu Windows). Domyślnie, Firefox i Thunderbird używa swojego własnego magazynu certyfikatów Mozilla zamiast magazynu certyfikatów systemu Windows. Jeśli program Kaspersky Security Center jest zainstalowany w Twojej organizacji, a zasada jest stosowana na komputerze, Kaspersky Endpoint Security automatycznie umożliwia korzystanie z magazynu certyfikatów w Firefox i Thunderbird, aby skanować ruch sieciowy tych aplikacji. Jeśli zasada nie jest stosowana na komputerze, możesz wybrać magazyn certyfikatów, który będzie używany przez aplikacje firmy Mozilla. Jeśli wybrano magazyn certyfikatów Mozilla, ręcznie dodaj do niego certyfikat Kaspersky. To pomoże uniknąć błędów podczas pracy z ruchem HTTPS.

Aby skanować ruch sieciowy w przeglądarce Mozilla Firefox i kliencie poczty Thunderbird, musisz [włączyć Skanowanie połączeń szyfrowanych](#). Jeśli Skanowanie połączeń szyfrowanych jest wyłączone, Kaspersky Endpoint Security nie skanuje ruchu sieciowego w przeglądarce Mozilla Firefox oraz w kliencie poczty Thunderbird.

Przed dodaniem certyfikatu do magazynu Mozilla, wyeksportuj certyfikat Kaspersky z Panelu sterowania Windows (właściwości przeglądarki). Więcej informacji na temat eksportowania certyfikatu Kaspersky można znaleźć w [Bazie wiedzy na stronie pomocy technicznej](#). Więcej informacji dotyczących dodawania certyfikatu do magazynu odwiedź [stronę internetową pomocy technicznej Mozilla](#).

Możesz wybrać magazyn certyfikatów tylko w lokalnym interfejsie aplikacji.


W celu wybrania magazynu certyfikatu do skanowania połączeń szyfrowania w Firefox i Thunderbird:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.
3. W sekcji **Mozilla Firefox i Thunderbird** zaznacz pole **Skanuj bezpieczny ruch sieciowy w aplikacjach Mozilla**.
4. Wybierz magazyn certyfikatów:
 - **Użyj magazynu certyfikatów systemu Windows.** Certyfikat główny Kaspersky zostanie dodany do tego magazynu podczas instalacji Kaspersky Endpoint Security.
 - **Użyj magazynu certyfikatów Mozilla.** Mozilla Firefox i Thunderbird używają swoich własnych magazynów certyfikatów. Jeśli wybrano magazyn certyfikatów aplikacji Mozilla, powinieneś ręcznie dodać certyfikat główny Kaspersky do tego magazynu z poziomu właściwości przeglądarki.
5. Zapisz swoje zmiany.

Wyłączanie połączeń szyfrowanych ze skanowania

Większość zasobów internetowych korzysta z połączeń szyfrowanych. Ekspersi z Kaspersky zalecają włączenie opcji [Skanowanie połączeń szyfrowanych](#). Jeśli skanowanie połączeń szyfrowanych zakłóca czynności związane z pracą, możesz dodać stronę internetową do wykluczeń zwanych *zaufanymi adresami*. Jeśli zaufana aplikacja korzysta z połączenia szyfrowanego, możesz [wyłączyć skanowanie połączeń szyfrowanych dla tej aplikacji](#). Na przykład, można wyłączyć skanowanie połączeń szyfrowanych w poszukiwaniu aplikacji do przechowywania w chmurze, które używają uwierzytelniania dwuskładnikowego z własnym certyfikatem.

W celu wykluczenia adresu internetowego ze skanowania połączeń szyfrowanych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.
3. W sekcji **Skanowanie połączeń szyfrowanych** kliknij przycisk **Zaufane adresy**.
4. Kliknij przycisk **Dodaj**.
5. Wprowadź nazwę domeny lub adres IP, jeśli nie chcesz, żeby Kaspersky Endpoint Security skanował połączenia szyfrowane nawiązywane podczas odwiedzania tej domeny.

Kaspersky Endpoint Security obsługuje znak  do wprowadzenia maski w nazwie domeny.

Kaspersky Endpoint Security nie obsługuje masek dla adresów IP. W lokalnym interfejsie aplikacji możesz wprowadzić zakres adresów IP (na przykład: 198.51.100.0/24). Zakresu adresów IP nie możesz wprowadzić w konsoli Kaspersky Security Center.


Na przykład:

- `domain.com` – wpis jest częścią następujących adresów: `https://domain.com`, `https://www.domain.com`, `https://domain.com/page123`. Wpis nie jest częścią poddomen (na przykład: `subdomain.domain.com`).
- `subdomain.domain.com` – wpis jest częścią następujących adresów: `https://subdomain.domain.com`, `https://subdomain.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`.
- `*.domain.com` – wpis jest częścią następujących adresów: `https://movies.domain.com`, `https://images.domain.com/page123`. Wpis nie jest częścią domeny `domain.com`.

6. Zapisz swoje zmiany.

Domyślnie Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych w przypadku wystąpienia błędów i dodaje stronę internetową do specjalnej listy *Domeny z błędami skanowania*. Kaspersky Endpoint Security tworzy osobną listę dla każdego użytkownika i nie wysyła danych do Kaspersky Security Center. Możesz [włączyć blokowanie połączenia, gdy wystąpi błąd skanowania](#). Możesz przejrzeć listę domen z błędami skanowania połączeń szyfrowanych tylko w lokalnym interfejsie aplikacji.

W celu wyświetlenia listy domen z błędami skanowania:


1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.

3. W sekcji **Skanowanie połączeń szyfrowanych** kliknij przycisk **Domeny z błędami skanowania**.

Zostanie otwarta lista domen z błędami skanowania. Aby zresetować listę, włącz blokowanie połączenia w przypadku wystąpienia błędów skanowania w zasadzie, zastosuj zasadę, a następnie zresetuj parametr do wartości początkowej i ponownie zastosuj zasadę.

Specjaliści z Kaspersky sporządzają listę *globalnych wykluczeń* – zaufanych stron internetowych, których Kaspersky Endpoint Security nie sprawdza niezależnie od ustawień aplikacji.

W celu przejrzania globalnych wykluczeń ze skanowania szyfrowanego ruchu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.
3. W sekcji **Skanowanie połączeń szyfrowanych** kliknij odnośnik do **stron internetowych**.

Spowoduje to otwarcie listy stron internetowych utworzonej przez ekspertów z Kaspersky. Kaspersky Endpoint Security nie skanuje chronionych połączeń dla stron internetowych na liście. Ta lista może zostać zaktualizowana, gdy zostaną zaktualizowane bazy danych i moduły Kaspersky Endpoint Security.

Kontrola komputera

Kontrola sieci

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Kontrola sieci zarządza dostępem użytkowników zasobów sieciowych. Pomaga to zmniejszyć ruch sieciowy i nieodpowiednie dysponowanie czasem pracy. Gdy użytkownik próbuje otworzyć stronę internetową ograniczoną przez Kontrolę sieci, Kaspersky Endpoint Security zablokuje dostęp lub wyświetli ostrzeżenie (patrz rysunek poniżej).

Kaspersky Endpoint Security monitoruje tylko ruch HTTP i HTTPS.

Dla monitorowania ruchu HTTPS należy [włączyć skanowanie zaszyfrowanych połączeń](#).

Metody zarządzania dostępem do stron internetowych

Kontrola sieci umożliwia konfigurowanie dostępu do stron internetowych przy użyciu następujących metod:

- **Kategoria strony internetowej.** Strony internetowe są kategoryzowane zgodnie z usługą chmury Kaspersky Security Network, analizą heurystyczną i bazą danych znanych stron internetowych (znajdującą się w bazach danych aplikacji). Na przykład, możesz ograniczyć dostęp użytkownika do kategorii „Sieci społecznościowe” lub do [innych kategorii](#).
- **Typ danych.** Na przykład, możesz ograniczyć dostęp użytkowników do danych na stronie internetowej i ukryć zawartość graficzną. Kaspersky Endpoint Security określa typ danych w oparciu o format pliku, a nie w oparciu o jego rozszerzenie.

Kaspersky Endpoint Security nie skanuje plików w archiwach. Na przykład, jeśli pliki obrazów zostały umieszczone w archiwum, Kaspersky Endpoint Security identyfikuje typ danych „Archiwa”, a nie „Pliki graficzne”.

- **Określony adres.** Możesz wprowadzić adres internetowy lub [użyć masek](#).

Możesz jednocześnie użyć kilku metod do regulowania dostępu do stron internetowych. Na przykład, możesz ograniczyć dostęp do typu danych „Pliki biurowe” tylko dla kategorii stron internetowych „Poczta przez WWW”.

Reguły dostępu do stron internetowych

Kontrola sieci zarządza dostępem użytkowników do stron internetowych przy użyciu *reguł dostępu*. Możesz skonfigurować następujące zaawansowane ustawienia reguły dostępu do stron internetowych:

- Użytkowników, do których stosowana jest reguła.

Na przykład, możesz ograniczyć dostęp do internetu poprzez przeglądarkę dla wszystkich użytkowników firmy, za wyjątkiem działu IT.

- Terminarz reguły.

Na przykład, możesz ograniczyć dostęp do internetu poprzez przeglądarkę tylko w trakcie godzin pracy.

Priorytety reguł dostępu

Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli strona internetowa została dodana do kilku reguł, Kontrola sieci reguluje dostęp do strony internetowej w oparciu o regułę z najwyższym priorytetem. Na przykład, Kaspersky Endpoint Security może identyfikować portal firmowy jako sieć społecznościową. Aby ograniczyć dostęp do sieci społecznościowych i zapewnić dostęp do firmowego portalu internetowego, utwórz dwie reguły: jedną regułę blokady dla kategorii stron internetowych „Sieci społecznościowe” i jedną regułę zezwalającą dla firmowego portalu internetowego. Reguła dostępu dla firmowego portalu internetowego musi posiadać wyższy priorytet niż reguła dostępu dla sieci społecznościowych.



Żądana strona internetowa nie może zostać wyświetlona.

Adres: <http://kaspersky.ru/>.

Strona internetowa została zablokowana zgodnie z regułą block.

Powód: zasób sieciowy należy do kategorii zawartości Nieokreślony i kategorii rodzaju danych Nieokreślony.

Ten zasób sieciowy jest zabroniony w firmie. Jeżeli uważasz, że zasób sieciowy został niesłusznie zablokowany lub potrzebujesz do niego dostęp, skontaktuj się z administratorem firmowej sieci lokalnej ([Poproś o dostęp](#)).

Komunikat wygenerowano: 10/29/2020 3:45:02 AM



Żądana strona może być niebezpieczna lub zabroniona przez politykę firmy.

Adres: <http://www.kaspersky.com/>.

Strona internetowa została zablokowana zgodnie z regułą warn.

Powód: zasób sieciowy należy do kategorii zawartości: Nieokreślony i kategorii rodzaju danych: Nieokreślony.

Kliknij odsyłacz <http://www.kaspersky.com/>, aby otworzyć tę stronę.
Aby uzyskać dostęp do całej zawartości strony, kliknij odsyłacz http://www.kaspersky.com/*.
Aby uzyskać dostęp do wszystkich istniejących domen należących do tego samego lub niższego poziomu z tą oznaczoną gwiazdką "*", kliknij odsyłacz */*.kaspersky.com/*.

Dostęp do wymienionych powyżej zasobów sieciowych zostanie przydzielony na czas trwania obecnej sesji Kaspersky Endpoint Security.


W przypadku pomyłkowego ostrzeżenia, skontaktuj się z administratorem firmowej sieci lokalnej ([Poproś o dostęp](#)).

Komunikat wygenerowano: 10/29/2020 3:44:55 AM

Włączanie i wyłączanie modułu Kontrola sieci

Domyślnie Kontrola sieci jest włączona.

W celu włączenia i wyłączenia modułu Kontrola sieci:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
3. Użyj przełącznika **Kontrola sieci**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

Działania podejmowane na regułach dostępu do zasobów sieciowych

Nie jest zalecane tworzenie więcej niż 1 000 reguł dostępu do zasobów internetowych, gdyż może to spowodować niestabilność systemu.

Reguła dostępu do zasobu sieciowego jest zestawem filtrów i działań, które program Kaspersky Endpoint Security wykonuje podczas odwiedzania przez użytkownika zasobów sieciowych opisanych w regule w przedziale czasu wskazanym w terminarzu reguły. Filtry umożliwiają dokładne określenie puli zasobów sieciowych, do których dostęp jest kontrolowany przez moduł Kontrola sieci.

Dostępne są następujące filtry:



- **Filtruj według zawartości.** Kontrola sieci kategoryzuje [zasoby sieciowe według zawartości](#) i typu danych. Możesz kontrolować dostęp użytkownika do zasobów sieciowych z zawartością i danymi należącymi do typów zdefiniowanych przez te kategorie. Podczas odwiedzania zasobów sieciowych należących do wybranej kategorii zawartości i / lub kategorii typu danych, program Kaspersky Endpoint Security wykonuje akcję określoną w regule.
- **Filtruj według adresów zasobów sieciowych.** Możesz kontrolować dostęp użytkownika do wszystkich adresów zasobów sieciowych lub do pojedynczego adresu zasobu sieciowego i / lub grup adresów zasobów sieciowych. Jeżeli wybrano filtrowanie według zawartości i filtrowanie według adresów zasobów sieciowych, a określone adresy zasobów sieciowych i / lub grupy adresów zasobów sieciowych należą do wybranej kategorii zawartości lub kategorii typu danych, program Kaspersky Endpoint Security nie będzie monitorował dostępu do wszystkich zasobów sieciowych w wybranej kategorii zawartości i / lub kategorii typu danych. Zamiast tego aplikacja będzie monitorowała dostęp tylko do określonych adresów zasobów sieciowych i / lub grup adresów zasobów sieciowych.
- **Filtruj według nazw użytkowników i grup użytkowników.** Możesz określić nazwy użytkowników i / lub grup użytkowników z dostępem do zasobów sieciowych, które są kontrolowane zgodnie z regułą.
- **Terminarz reguły.** Możesz określić terminarz reguły. Terminarz reguły określa przedział czasu, podczas którego Kaspersky Endpoint Security monitoruje dostęp do zasobów sieciowych, dla których stosowana jest reguła.

Po zainstalowaniu Kaspersky Endpoint Security lista reguł modułu Kontrola sieci nie jest pusta. Znajdują się na niej dwie reguły:

- Reguła Skrypty i arkusze stylów, która nadaje wszystkim użytkownikom uprawnienia dostępu do zasobów sieciowych, których adresy zawierają nazwy plików z rozszerzeniami CSS, JS lub VBS, w dowolnym czasie. Na przykład: <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.
- Reguła domyślna. Ta reguła jest stosowana do wszelkich zasobów internetowych, które nie są objęte innymi regułami, i zezwala na lub blokuje dostęp do tych zasobów internetowych wszystkim użytkownikom.

Dodawanie reguły dostępu do zasobu sieciowego

W celu dodania lub zmodyfikowania reguły dostępu do zasobu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
3. W sekcji **Ustawienia** kliknij przycisk **Reguła dostępu do zasobów sieciowych**.
4. W oknie kliknij przycisk **Dodaj**.
Zostanie otwarte okno **Reguła dostępu do zasobów sieciowych**.
5. W polu **Nazwa reguły** wprowadź nazwę reguły.
6. Wybierz stan **Aktywny** dla reguły dostępu do zasobu internetowego.
Możesz użyć przełącznika do [wyłączenia reguły dostępu do zasobu sieciowego](#) w dowolnym momencie.
7. W sekcji **Akcja** zaznacz odpowiednią opcję:
 - **Zezwól**. Jeśli wybrano tę wartość, Kaspersky Endpoint Security zezwala na dostęp do zasobu sieciowego odpowiadającego ustawieniom reguły.
 - **Blokuj**. Jeśli wybrano tę wartość, Kaspersky Endpoint Security blokuje dostęp do zasobu sieciowego odpowiadającego ustawieniom reguły.
 - **Ostrzegaj**. Jeśli wybrano tę wartość, przy próbie uzyskania przez użytkownika dostępu do zasobu sieciowego odpowiadającego parametrom reguły, Kaspersky Endpoint Security wyświetla wiadomość ostrzegającą o niepożądanym zasobie sieciowym. Korzystając z odnośników znajdujących się w wiadomości ostrzegającej, użytkownik może uzyskać dostęp do żądanego zasobu sieciowego.
8. W sekcji **Filtrowanie zawartości** wybierz odpowiedni filtr zawartości:
 - **Według kategorii zawartości**. Możesz kontrolować dostęp użytkownika do zasobów internetowych według [kategorii](#)  (na przykład: kategoria *Sieci społecznościowe*).
 - **Według typu danych**. Możesz kontrolować dostęp użytkownika do zasobów internetowych w oparciu o określony typ danych opublikowanych w nich danych (na przykład: *Obrazy graficzne*).

W celu skonfigurowania filtra zawartości:

- a. Kliknij odnośnik **Konfiguruj**.
- b. Zaznacz pola obok nazw wymaganych kategorii zawartości i / lub kategorii typu danych.

Zaznaczenie pola obok nazwy kategorii zawartości i / lub kategorii typu danych oznacza, że Kaspersky Endpoint Security będzie stosować regułę kontrolowania dostępu do zasobów sieciowych należących do wybranych kategorii zawartości i / lub kategorii typu danych.

c. Wróć do okna konfiguracji reguły dostępu do zasobu internetowego.

9. W sekcji **Adresy** wybierz odpowiedni filtr adresu zasobu internetowego:

- **Dla wszystkich adresów.** Kontrola sieci nie będzie filtrowała zasobów sieciowych według adresu.
- **Dla określonych adresów.** Kontrola sieci będzie filtrowała tylko adresy zasobów internetowych z listy. W celu utworzenia listy adresów zasobów internetowych:

a. Kliknij przycisk **Dodaj adres** lub **Dodaj grupę adresów**.

b. W otwartym oknie utwórz listę adresów zasobów internetowych. Możesz wprowadzić adres internetowy lub [użyć masek](#). Możesz także [wyeksportować listę adresów zasobów internetowych z pliku TXT](#).

c. Wróć do okna konfiguracji reguły dostępu do zasobu internetowego.

Jeśli [Skanowanie połączeń szyfrowanych jest wyłączone](#), dla protokołu HTTPS możesz filtrować tylko według nazwy serwera.

10. W sekcji **Użytkownicy** wybierz odpowiedni filtr dla użytkowników:

- **Dla wszystkich użytkowników.** Kontrola sieci nie będzie filtrowała zasobów sieciowych dla określonych użytkowników.
- **Dla użytkowników indywidualnych i/lub grup.** Kontrola sieci będzie filtrowała zasoby internetowe tylko dla określonych użytkowników. W celu utworzenia listy użytkowników, do których chcesz zastosować regułę:

a. Kliknij przycisk **Dodaj**.

b. W otwartym oknie wybierz użytkowników lub grupy użytkowników, do których chcesz zastosować regułę dostępu do zasobu sieciowego.

c. Wróć do okna konfiguracji reguły dostępu do zasobu internetowego.

11. Z otwartej listy rozwijalnej **Terminarz reguły** wybierz żądany terminarz lub utwórz nowy oparty na wybranym terminarzu reguły. W tym celu:

a. Kliknij przycisk **Edytuj lub dodaj nowy**.

b. W oknie kliknij przycisk **Dodaj**.

c. W otwartym oknie wprowadź nazwę terminarza reguły.

d. Konfiguruj terminarz dostępu do zasobu sieciowego dla użytkowników.


e. Wróć do okna konfiguracji reguły dostępu do zasobu internetowego.

12. Zapisz swoje zmiany.

Przydzielanie priorytetów do reguł dostępu do zasobów sieciowych


Możesz przydzielić priorytet do każdej reguły z listy reguł, zmieniając ich kolejność na liście.

W celu przydzielenia priorytetu regule dostępu do zasobu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
3. W sekcji **Ustawienia** kliknij przycisk **Reguła dostępu do zasobów sieciowych**.
4. W otwartym oknie wybierz regułę, której priorytet chcesz zmienić.
5. Użyj przycisków **W górę** i **W dół** w celu przesunięcia reguły na odpowiednią pozycję na liście reguł dostępu do zasobów internetowych.
6. Zapisz swoje zmiany.

Włączanie i wyłączanie reguły dostępu do zasobu sieciowego

W celu włączenia lub wyłączenia reguły dostępu do zasobu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
3. W sekcji **Ustawienia** kliknij przycisk **Reguła dostępu do zasobów sieciowych**.
4. W otwartym oknie wybierz regułę, którą chcesz włączyć lub wyłączyć.
5. W kolumnie **Stan** wykonaj następujące czynności:
 - Jeżeli chcesz włączyć regułę, wybierz wartość **Aktywna**.
 - Jeżeli chcesz wyłączyć regułę, wybierz wartość **Nieaktywna**.
6. Zapisz swoje zmiany.

Eksportowanie i importowanie listy zaufanych adresów internetowych

Możesz wyeksportować listę reguł Kontroli sieci do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę adresów tego samego typu. Możesz użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy reguł Kontroli sieci lub przeniesienia listy na inny serwer.

[Jak w Konsoli administracyjnej \(MMC\) wyeksportować i zaimportować listę reguł Kontroli sieci?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
6. W celu wyeksportowania listy reguł Kontroli sieci:
 - a. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.
7. W celu zaimportowania listy reguł Kontroli sieci:
 - a. Kliknij odnośnik **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
 - b. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.


[Jak w konsoli Web Console i Cloud Console wyeksportować i zaimportować listę reguł Kontroli sieci?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listę reguł.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Kontrola zabezpieczeń** → **Kontrola sieci**.
5. W celu wyeksportowania listy reguł w sekcji **Lista reguł**:
 - a. Wybierz reguły, które chcesz zmienić.
 - b. Kliknij przycisk **Eksportuj**.
 - c. Potwierdź chęć wyeksportowania tylko wybranych reguł lub wyeksportuj całą listę.
 - d. Kliknij przycisk **Eksportuj**.
Kaspersky Endpoint Security eksportuje listę reguł do pliku XML w domyślnym folderze do pobrania.
6. W celu zaimportowania listy reguł w sekcji **Lista reguł**:
 - a. Kliknij odnośnik **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
 - b. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
7. Zapisz swoje zmiany.

Testowanie reguł dostępu do zasobów sieciowych

Aby sprawdzić działanie reguł Kontroli sieci, możesz je przetestować. Do tego celu moduł Kontrola sieci zawiera funkcję Diagnostyka reguł.

W celu przetestowania reguły dostępu do zasobu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
3. W sekcji **Ustawienia** kliknij odnośnik **Diagnostyka reguł**.
Zostanie otwarte okno **Diagnostyka reguł**.
4. Jeśli chcesz przetestować reguły wykorzystywane przez Kaspersky Endpoint Security do kontrolowania dostępu do określonego zasobu sieciowego, zaznacz pole **Określ adres**. W polu poniżej wprowadź adres zasobu sieciowego.


5. Jeśli chcesz przetestować reguły wykorzystywane przez Kaspersky Endpoint Security do kontrolowania dostępu do zasobów sieciowych dla określonych użytkowników i / lub grup użytkowników, określ listę użytkowników i / lub grup użytkowników.
6. Jeśli chcesz przetestować reguły wykorzystywane przez Kaspersky Endpoint Security do kontrolowania dostępu do zasobów sieciowych o pewnych kategoriach zawartości i/lub kategoriach typu danych, zaznacz pole **Filtrowanie zawartości** i wybierz odpowiednią opcję z listy rozwijalnej (**Według kategorii zawartości**, **Według typu danych** lub **Według kategorii zawartości i typu danych**).
7. Jeśli chcesz przetestować reguły biorąc pod uwagę godzinę i dzień tygodnia, w którym podejmowana jest próba uzyskania dostępu do zasobów sieciowych określonych w warunkach diagnostyki, zaznacz pole **Uwzględnij czas próby dostępu**. Następnie określ dzień tygodnia i czas.
8. Kliknij przycisk **Skanuj**.

Po zakończeniu testu wyświetlana jest wiadomość o akcji podjętej przez Kaspersky Endpoint Security, zgodnie z pierwszą regułą wyzwoloną przy próbie dostępu do określonego zasobu sieciowego (akceptuj, zablokuj lub ostrzeżenie). Pierwsza wyzwolona reguła to ta zajmująca wyższą pozycję na liście reguł Kontroli sieci niż reszta reguł spełniających warunki diagnostyki. Wiadomość jest wyświetlana po prawej stronie przycisku **Skanuj**. Następująca tabela wyświetla pozostałe wyzwolone reguły, określając akcję wykonaną przez Kaspersky Endpoint Security. Reguły uszeregowane są malejąco według priorytetu.

Eksportowanie i importowanie listy adresów zasobów sieciowych

Jeżeli w regule dostępu do zasobu sieciowego utworzyłeś listę adresów zasobów sieciowych, będziesz mógł ją wyeksportować do pliku .txt. Możliwe będzie również zaimportowanie listy z tego pliku, dzięki czemu podczas konfigurowania reguły dostępu nie będzie konieczne tworzenie nowej listy. Opcja eksportowania i importowania listy adresów dostępu do zasobów sieciowych jest użyteczna, gdy, na przykład, tworzysz reguły dostępu z tymi samymi parametrami.

W celu zaimportowania lub wyeksportowania listy adresów zasobów sieciowych do pliku:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
3. W sekcji **Ustawienia** kliknij przycisk **Reguła dostępu do zasobów sieciowych**.
4. Wybierz regułę, której listę adresów zasobów sieciowych chcesz wyeksportować lub zaimportować.
5. W celu wyeksportowania listy zaufanych adresów sieciowych, w sekcji **Adresy** wykonaj następujące czynności:
 - a. Wybierz adresy, które chcesz wyeksportować.
Jeśli nie wybrałeś żadnego adresu, Kaspersky Endpoint Security wyeksportuje wszystkie adresy.
 - b. Kliknij przycisk **Eksportuj**.
 - c. W otwartym oknie wprowadź nazwę pliku TXT, do którego chcesz wyeksportować listę adresów zasobów internetowych i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje listę adresów zasobów internetowych do pliku TXT.
6. W celu zaimportowania listy zasobów sieciowych, w sekcji **Adresy** wykonaj następujące czynności:

a. Kliknij przycisk **Importuj**.

W oknie, które zostanie otwarte, wybierz plik TXT, z którego chcesz zaimportować listę zasobów sieciowych.

b. Kliknij przycisk **Otwórz**.




Jeśli komputer ma już listę zaufanych adresów, Kaspersky Endpoint Security wyświetli monit o usunięciu istniejącej listy lub dodanie do niej nowych wpisów z pliku TXT.

7. Zapisz swoje zmiany.

Monitorowanie aktywności użytkownika w internecie

Kaspersky Endpoint Security umożliwia zapisywanie danych dotyczących odwiedzin użytkownika na wszystkich stronach internetowych, w tym dozwolonych stronach internetowych. Umożliwia to uzyskanie pełnej historii wyświetleń przeglądarki. Kaspersky Endpoint Security wysyła zdarzenia dotyczące aktywności użytkownika do Kaspersky Security Center, do [lokalnego raportu Kaspersky Endpoint Security](#), a także do dziennika zdarzeń systemu Windows. Aby uzyskać zdarzenia w Kaspersky Security Center, należy skonfigurować ustawienia zdarzeń w zasadzie w Konsoli administracyjnej lub w Web Console. Można także skonfigurować przesyłanie zdarzeń Web Control za pośrednictwem poczty elektronicznej oraz wyświetlanie powiadomień na komputerze użytkownika.


Kaspersky Endpoint Security tworzy następujące zdarzenia aktywności użytkownika w internecie:

- Blokowanie stron internetowych (stan *Zdarzenia krytyczne* .
- Wizyta na niezalecanej stronie internetowej (stan *Ostrzeżenia* .
- Odwiedzenie dozwolonej strony internetowej (stan *Wiadomości informacyjne* .

Przed włączeniem monitorowania aktywności użytkownika w internecie należy wykonać następujące czynności:

- Wstrzykuj skrypt do ruchu sieciowego w celu interakcji ze stronami sieciowymi (patrz instrukcje poniżej). Skrypt włącza rejestrację zdarzeń Kontroli sieci.
- Dla monitorowania ruchu HTTPS należy [włączyć skanowanie zaszyfrowanych połączeń](#).

W celu wstrzyknięcia skryptu interakcji ze stronami internetowymi do ruchu sieciowego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.
3. W sekcji **Przetwarzanie ruchu sieciowego** zaznacz pole **Wstrzykuj skrypt do ruchu sieciowego w celu interakcji ze stronami internetowymi**.
4. Zapisz swoje zmiany.

W rezultacie Kaspersky Endpoint Security wstrzyknie skrypt interakcji ze stronami internetowymi do ruchu sieciowego. Ten skrypt umożliwia rejestrację zdarzeń Kontroli sieci dla dziennika zdarzeń aplikacji, dziennika zdarzeń systemu operacyjnego i [raportów](#).

W celu skonfigurowania rejestrowania zdarzeń Kontroli sieci na komputerze użytkownika:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Interfejs**.

3. W sekcji **Powiadomienia** kliknij **Ustawienia powiadomień**.

4. W otwartym oknie wybierz sekcję **Kontrola sieci**.

Spowoduje to otwarcie tabeli zdarzeń Kontroli sieci i metod powiadamiania.

5. Skonfiguruj metodę powiadamiania dla każdego zdarzenia: **Zapisz w raporcie lokalnym** lub **Zapisz w dzienniku zdarzeń Windows**.

Aby zapisywać zdarzenia dotyczące odwiedzania dozwolonych stron internetowych, należy skonfigurować Kontrolę sieci (zapoznaj się z poniższymi instrukcjami).

W tabeli zdarzeń można także włączyć powiadomienia ekranowe i powiadomienia e-mail. Aby powiadomienia były wysyłane w wiadomościach e-mail, należy skonfigurować ustawienia serwera SMTP. Więcej informacji o wysyłaniu powiadomień za pośrednictwem poczty elektronicznej znajdziesz w [pomocy do Kaspersky Security Center](#).

6. Zapisz swoje zmiany.

W wyniku tego Kaspersky Endpoint Security rozpocznie rejestrowanie zdarzeń dotyczących aktywności użytkownika w internecie.

Kontrola sieci wysyła zdarzenia aktywności użytkownika do Kaspersky Security Center w następujący sposób:

- Jeśli używasz Kaspersky Security Center, Kontrola sieci wysyła zdarzenia dla wszystkich obiektów tworzących stronę internetową. Z tego powodu kilka zdarzeń może zostać utworzonych po zablokowaniu strony. Na przykład, podczas blokowania strony <http://www.example.com>, Kaspersky Endpoint Security może przesłać zdarzenia dla następujących obiektów: <http://www.example.com>, <http://www.example.com/icon.ico>, <http://www.example.com/file.js> itd.
- Jeśli korzystasz z Kaspersky Security Center Cloud Console, Kontrola sieci grupuje zdarzenia i wysyła tylko protokół i domenę witryny. Na przykład, jeśli użytkownik otworzy niechciane strony internetowe <http://www.example.com/main>, <http://www.example.com/contact> i <http://www.example.com/gallery>, Kaspersky Endpoint Security wyśle tylko jedno zdarzenie z obiektem <http://www.example.com>.

W celu włączenia zapisywania zdarzeń dotyczących odwiedzania dozwolonych stron internetowych:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.

3. W sekcji **Dodatkowe** kliknij przycisk **Ustawienia zaawansowane**.

4. W otwartym oknie zaznacz pole **Zapisuj informacje o otwarciu dozwolonych stron**.

5. Zapisz swoje zmiany.

W rezultacie możliwe będzie przejrzanie całej historii przeglądania.

Modyfikowanie szablonów wiadomości Kontroli sieci

W zależności od typu akcji określonej we właściwościach reguł Kontroli sieci, przy próbie dostępu użytkowników do zasobów internetowych Kaspersky Endpoint Security wyświetla wiadomość o jednym z następujących typów (zamiast odpowiedzi serwera HTTP aplikacja dostarcza stronę HTML z wiadomością):

- **Ostrzeżenie.** Taka wiadomość ostrzega użytkownika, że odwiedzenie zasobu sieciowego nie jest zalecane i/lub narusza politykę bezpieczeństwa firmy. Kaspersky Endpoint Security wyświetla ostrzeżenie, jeśli z listy rozwijalnej **Akcja**, dostępnej w ustawieniach reguły opisującej zasób sieciowy, wybrano opcję **Ostrzegaj**.


Jeśli użytkownik sądzi, że ostrzeżenie jest pomyłką, może kliknąć odnośnik w ostrzeżeniu w celu wysłania wcześniej wygenerowanej wiadomości do administratora lokalnej sieci firmowej.

- **Wiadomość informująca o zablokowaniu zasobu sieciowego.** Kaspersky Endpoint Security wyświetla wiadomość informującą o zablokowaniu zasobu, jeśli z listy rozwijalnej **Akcja**, dostępnej w ustawieniach reguły opisującej zasób sieciowy, wybrano opcję **Zablokuj**.

Jeśli użytkownik sądzi, że zasób sieciowy został zablokowany przez pomyłkę, może kliknąć odnośnik w wiadomości informującej o zablokowaniu zasobu sieciowego w celu wysłania wcześniej wygenerowanej wiadomości do administratora lokalnej sieci firmowej.

Dostępne są specjalne szablony dla wiadomości ostrzegającej, informującej o zablokowaniu zasobu sieciowego i zgłoszenia wysłanego do administratora sieci LAN. Możesz zmodyfikować ich zawartość.

W celu zmodyfikowania szablonu dla wiadomości Kontroli sieci:


1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola sieci**.
3. W sekcji **Szablony** skonfiguruj szablony dla wiadomości Kontroli sieci:
 - **Ostrzeżenie.** Pole do wprowadzenia danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła ostrzegająca o próbach uzyskania dostępu do niechcianych zasobów sieciowych.
 - **Wiadomość dotycząca blokowania.** To pole do wprowadzania danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła blokująca dostęp do zasobu sieciowego.
 - **Wiadomość do administratora.** Szablon wiadomości wysyłanej do administratora sieci LAN, gdy użytkownik uważa blokadę za pomyłkę. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania dostępu do strony internetowej** Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkowników**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.
4. Zapisz swoje zmiany.

Modyfikowanie masek adresów zasobów sieciowych

Korzystanie z *maski adresu zasobu sieciowego* (nazywanej również "maską adresu") może być użyteczne, gdy podczas tworzenia reguły dostępu do zasobu sieciowego wprowadzasz kilka podobnych adresów zasobów sieciowych. Jedna maska adresu może odpowiadać większej liczbie adresów zasobów sieciowych.

Podczas tworzenia maski adresu postępuj zgodnie z następującymi regułami:

1. Symbol  zastępuje dowolną sekwencję zawierającą zero lub więcej znaków.

Na przykład, gdy wprowadzisz maskę adresu , reguła dostępu będzie stosowana do wszystkich zasobów sieciowych zawierających sekwencję znaków `abc`. Na przykład: `http://www.example.com/page_0-9abcdef.html`.

2. Sekwencja znaków `*.` (znana jako *maska domeny*) umożliwia wybranie wszystkich domen adresu. Maską domeny `*.` reprezentuje dowolną nazwę domeny, nazwę poddomeny lub pusty wiersz.

Na przykład: maska `*.example.com` reprezentuje następujące adresy:

- `http://pictures.example.com`. Maską domeny `*.` reprezentuje `pictures.`
- `http://user.pictures.example.com`. Maską domeny `*.` reprezentuje `pictures.` i `user.`
- `http://example.com`. Maską domeny `*.` Jest interpretowana jako pusty wiersz.

3. Sekwencja znaków `www.` na początku maski adresu jest interpretowana jako sekwencja `*.`

Przykład: maska adresu `www.example.com` jest traktowana jako `*.example.com`. Ta maska obejmuje adresy `www2.example.com` i `www.pictures.example.com`.

4. Jeżeli maska adresu nie rozpoczyna się od znaku `*`, wówczas zawartość maski adresu będzie odpowiadała tej samej zawartości z przedrostkiem `*.`

5. Jeśli maska adresu kończy się znakiem innym niż `/` lub `*`, zawartość maski adresu jest traktowana jak ta sama zawartość z przyrostkiem `/*`.

Na przykład: maska adresu `http://www.example.com` odpowiada adresowi `http://www.example.com/abc`, gdzie a, b i c są dowolnymi znakami.

6. Jeżeli maska adresu kończy się znakiem `/`, wówczas zawartość maski adresu będzie odpowiadała tej samej zawartości z przyrostkiem `/*`.

7. Sekwencja znaku `/*` na końcu maski adresu jest interpretowana jako `/*` lub pusty ciąg znaków.

8. Adresy zasobów sieciowych są weryfikowane na podstawie maski adresu z uwzględnieniem protokołu (`http` lub `https`):

- Jeżeli maska adresu nie zawiera protokołu sieciowego, będzie ona odpowiadała adresom z dowolnym protokołem sieciowym.

Przykład: maska adresu `example.com` obejmuje adresy `http://example.com` i `https://example.com`.

- Jeżeli maska adresu zawiera protokół sieciowy, będzie ona odpowiadała tylko adresowi z tym samym protokołem sieciowym.

Na przykład: maska adresu `http://*.example.com` odpowiada adresowi `http://www.example.com`, ale nie adresowi `https://www.example.com`.

9. Maskę adresu podaną w podwójnych cudzysłowach jest przetwarzana bez brania pod uwagę dodatkowych zamienników, za wyjątkiem znaku `*`, jeśli został włączony w skład maski adresu. Reguły 5 i 7 nie są stosowane do masek adresów umieszczonych w podwójnym cudzysłowie (przykłady 14 – 18 w tabeli poniżej).

10. Podczas porównywania z maską adresu zasobu sieciowego nie jest brana pod uwagę nazwa użytkownika i hasło, port połączenia oraz wielkość znaków.

Przykłady użycia reguł tworzenia masek adresów

Nr	Maska adresu	Sprawdzany adres zasobu sieciowego	Zastępowanie adresu przez maskę adresu	Komentarz
1	<code>*.example.com</code>	<code>http://www.123example.com</code>	Nie	Patrz reguła 1.
2	<code>*.example.com</code>	<code>http://www.123.example.com</code>	Tak	Patrz reguła 2.

3	*example.com	http://www.123example.com	Tak	Patrz reguła 1.
4	*example.com	http://www.123.example.com	Tak	Patrz reguła 1.
5	http://www.*.example.com	http://www.123example.com	Nie	Patrz reguła 1.
6	www.example.com	http://www.example.com	Tak	Patrz reguły 3, 2, 1.
7	www.example.com	https://www.example.com	Tak	Patrz reguły 3, 2, 1.
8	http://www.*.example.com	http://123.example.com	Tak	Patrz reguły 3, 4, 1.
9	www.example.com	http://www.example.com/abc	Tak	Patrz reguły 3, 5, 1.
10	example.com	http://www.example.com	Tak	Patrz reguły 3, 1.
11	http://example.com/	http://example.com/abc	Tak	Patrz reguła 6.
12	http://example.com/*	http://example.com	Tak	Patrz reguła 7.
13	http://example.com	https://example.com	Nie	Patrz reguła 8.
14	"example.com"	http://www.example.com	Nie	Patrz reguła 9.
15	"http://www.example.com"	http://www.example.com/abc	Nie	Patrz reguła 9.
16	"*.example.com"	http://www.example.com	Tak	Patrz reguły 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Tak	Patrz reguły 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Tak	Patrz reguły 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Nie	Maska adresu zawiera więcej informacji niż adres zasobu sieciowego.

Przenoszenie reguł dostępu do zasobów sieciowych z poprzedniej wersji aplikacji

Jeśli Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub poprzednia wersja aplikacji jest aktualizowana do Kaspersky Endpoint Security for Windows 11.7.0, reguły dostępu do zasobów sieciowych oparte o kategorie zawartości zasobów sieciowych zostają przeniesione zgodnie z następującymi zasadami:

- Reguły dostępu do zasobów sieciowych oparte o jedną lub kilka kategorii zawartości zasobów sieciowych z list „Czaty i fora”, „Poczta przez WWW” i „Sieci społecznościowe” zostają przeniesione do kategorii „Komunikacja przez internet”.
- Reguły dostępu do zasobów sieciowych oparte o jedną lub kilka kategorii zawartości zasobów sieciowych z list „Sklepy internetowe” i „Systemy płatności” zostają przeniesione do kategorii „Sklepy internetowe, banki, systemy płatności”.
- Reguły dostępu do zasobów sieciowych oparte o kategorię zawartości zasobów sieciowych "Hazard" zostają przeniesione do kategorii "Hazard, loterie, zakłady bukmacherskie".
- Reguły dostępu do zasobów sieciowych oparte o kategorię zawartości zasobów sieciowych "Gry przeglądarkowe" zostają przeniesione do kategorii "Gry komputerowe".

- Reguły dostępu do zasobów sieciowych oparte o kategorię zawartości zasobów sieciowych, które nie zostały wymienione powyżej, zostają przeniesione bez żadnych zmian.

Kontrola urządzeń

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Kontrola urządzeń zarządza dostępem użytkownika do urządzeń, które są instalowane na komputerze lub są podłączone do komputera (na przykład: dyski twarde, kamery lub moduły Wi-Fi). Umożliwia to ochronę komputera przed infekcją, gdy takie urządzenia są podłączone, oraz zapobieganie utracie lub wyciekowi danych.

Poziomy dostępu do urządzenia

Kontrola urządzeń kontroluje dostęp na następujących poziomach:

- **Typ urządzenia.** Na przykład: drukarki, dyski wymienne oraz płyty CD/DVD.

Dostęp urządzenia możesz skonfigurować w następujący sposób:

- Zezwól – ✓.
- Zablokuj – ✗.
- Zależy od magistrali połączeń (za wyjątkiem Wi-Fi) – 🌈.
- Blokuje z wyjątkami (tylko Wi-Fi) – 📄.

- **Magistrala połączeń.** *Magistrala połączeń* to interfejs używany do podłączania urządzeń do komputera (na przykład: USB lub FireWire). Dlatego możesz ograniczyć podłączenie wszystkich urządzeń, na przykład, za pośrednictwem USB.

Dostęp urządzenia możesz skonfigurować w następujący sposób:

- Zezwól – ✓.
- Zablokuj – ✗.

- **Zaufane urządzenia.** *Zaufane urządzenia* są urządzeniami, do których użytkownicy, określani w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

Możesz dodać zaufane urządzenia w oparciu o następujące dane:

- **Urządzenia według ID.** Każde urządzenie posiada unikatowy identyfikator (identyfikator sprzętu lub HWID). Możesz sprawdzić identyfikator we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Przykładowy identyfikator urządzenia: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Dodawanie urządzeń według identyfikatora jest wygodne, jeśli chcesz dodać kilka określonych urządzeń.
- **Urządzenia według modelu.** Każde urządzenie posiada identyfikator producenta (VID) oraz identyfikator produktu (PID). Możesz sprawdzić identyfikatory we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Szablon do wprowadzenia VID i PID: `VID_1234&PID_5678`. Dodawanie urządzeń

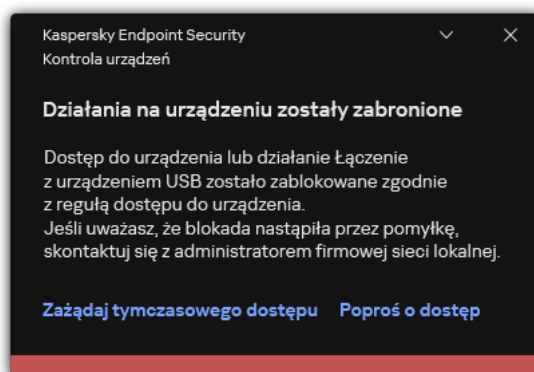
według modelu jest wygodne, jeśli w swojej organizacji używasz urządzeń pewnego modelu. W ten sposób możesz dodać wszystkie urządzenia tego modelu.

- **Urządzenia według maski ID.** Jeśli używasz kilku urządzeń z podobnymi identyfikatorami, możesz dodać urządzenia do listy zaufanych, korzystając z maski. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład: `WDC_C*`.
- **Urządzenia według maski modelu.** Jeśli używasz kilku urządzeń z podobnymi numerami VID lub PID (na przykład, urządzeń od tego samego producenta), możesz dodać urządzenia do listy zaufanych przy użyciu masek. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład: `VID_05AC & PID_*`.

Kontrola urządzeń reguluje dostęp użytkownika do urządzeń przy użyciu [reguły dostępu](#). Kontrola urządzeń umożliwia także zapisywanie zdarzeń podłączenia/odłączenia urządzenia. Aby zapisać zdarzenia, musisz skonfigurować rejestrację zdarzeń w profilu.

Jeśli dostęp do urządzenia zależy od magistrali połączenia (stan 🌈), Kaspersky Endpoint Security nie zapisuje zdarzeń podłączenia/odłączenia urządzenia. Aby umożliwić Kaspersky Endpoint Security zapisywanie zdarzeń podłączenia/odłączenia urządzenia, zezwól na dostęp do odpowiedniego typu urządzenia (stan ✓) lub dodaj urządzenie do listy zaufanych.

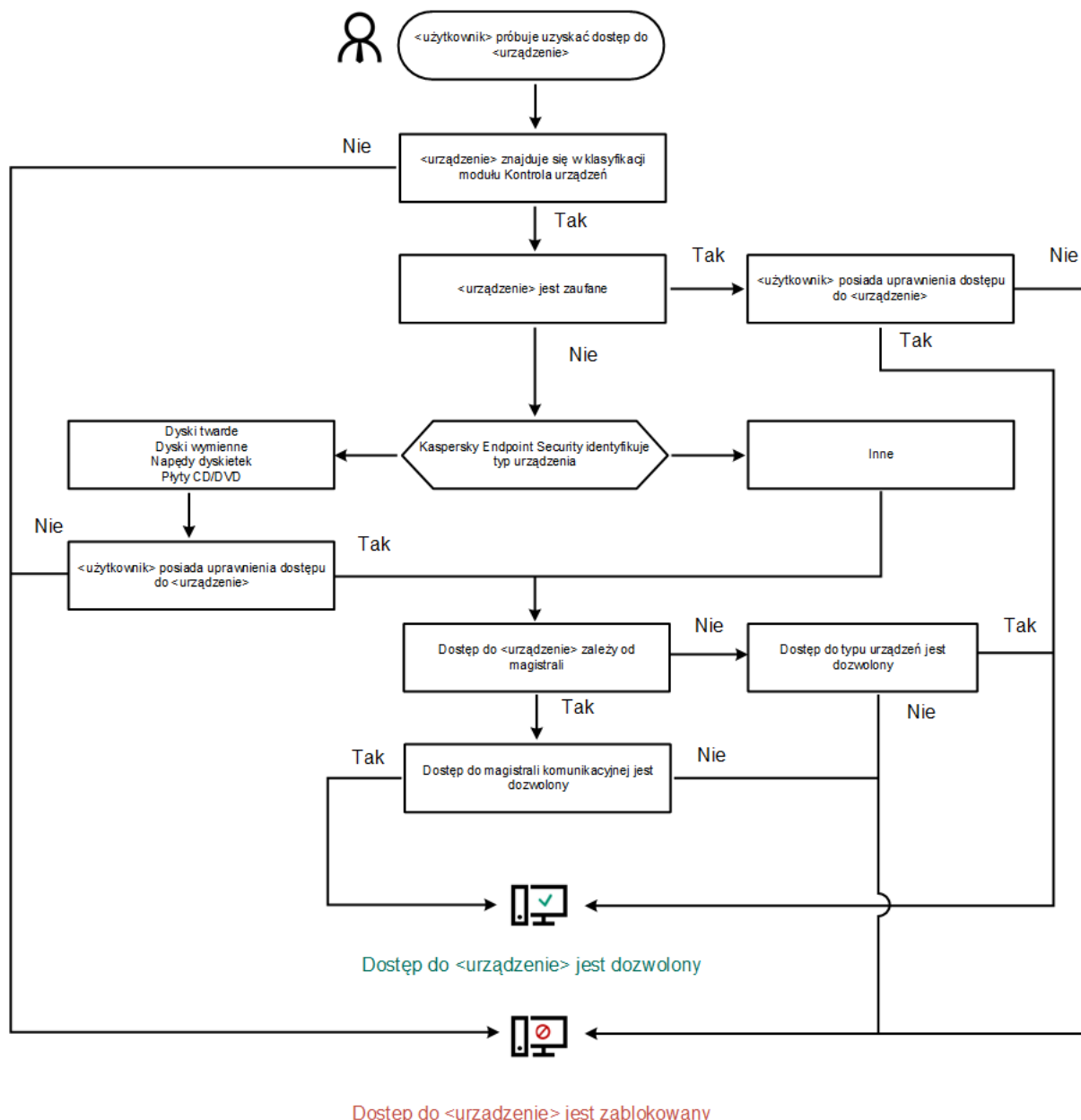
Jeśli urządzenie, które jest zablokowane przez Kontrolę urządzeń, zostanie podłączone do komputera, Kaspersky Endpoint Security zablokuje dostęp i wyświetli komunikat (patrz rysunek poniżej).



Komunikat Kontroli urządzeń

Algorytm działania Kontroli urządzeń

Kaspersky Endpoint Security podejmuje decyzję dotyczącą zezwolenia na dostęp do urządzenia po podłączeniu urządzenia do komputera przez użytkownika (patrz rysunek poniżej).



Dostęp do <urządzenie> jest zablokowany

Algorytm działania Kontroli urządzeń

Jeśli urządzenie jest podłączone i dostęp jest dozwolony, możesz edytować regułę dostępu i zablokować dostęp. W tym przypadku, kolejnym razem, gdy ktoś spróbuje uzyskać dostęp do urządzenia (np. przejrzeć drzewo folderów lub wykonać operacje odczytu lub zapisu), Kaspersky Endpoint Security zablokuje dostęp. Urządzenie bez systemu plików jest blokowane dopiero przy następnym podłączeniu.

Jeśli użytkownik komputera, na którym jest zainstalowany program Kaspersky Endpoint Security, poprosi o dostęp do urządzenia, które uważa, że zostało zablokowane przez pomyłkę, wyślij do użytkownika [instrukcje wysyłania pliku żądania dostępu](#).

Włączanie i wyłączanie modułu Kontrola urządzeń

Domyślnie Kontrola urządzeń jest włączona.

W celu włączenia lub wyłączenia modułu Kontrola urządzeń:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.

3. Użyj przełącznika **Kontrola urządzeń**, aby włączyć lub wyłączyć komponent.

4. Zapisz swoje zmiany.

W wyniku tego działania, jeśli moduł Kontrola urządzenia jest włączony, aplikacja przekazuje informacje o podłączonych urządzeniach do Kaspersky Security Center. Listę podłączonych urządzeń można przejrzeć w Kaspersky Security Center, w folderze **Sprzęt**.

Informacje o regułach dostępu

Reguły dostępu obejmują grupy ustawień, które określają, którzy użytkownicy mogą uzyskać dostęp do urządzeń zainstalowanych na lub podłączonych do komputera. Nie możesz dodać urządzenia, które znajduje się poza klasyfikacją Kontroli urządzeń. Dostęp do takich urządzeń jest dozwolony dla wszystkich użytkowników.

Reguły dostępu do urządzenia

Grupa ustawień dla reguły dostępu różni się w zależności od typu urządzenia (patrz tabela poniżej).

Ustawienia reguły dostępu



Urządzenia	Kontrola dostępu	Terminarz dostępu do urządzenia	Przydzielanie użytkowników i/lub grup użytkowników	Priorytet	Uprawnienie do odczytu/zapisu
Dyski twarde	✓	✓	✓	✓	✓
Dyski wymienne	✓	✓	✓	✓	✓
Drukarki	✓	–	–	–	–
Napędy dyskietek	✓	✓	✓	✓	✓
Płyty CD/DVD	✓	✓	✓	✓	✓
Modemy	✓	–	–	–	–
Urządzenia taśmowe	✓	–	–	–	–
Urządzenia wielofunkcyjne	✓	–	–	–	–
Czytniki kart inteligentnych	✓	–	–	–	–
Urządzenia Windows CE USB ActiveSync	✓	–	–	–	–
Zewnętrzne karty sieciowe	✓	–	–	–	–
Urządzenia przenośne (MTP)	✓	✓	✓	✓	✓
Bluetooth	✓	–	–	–	–


Aparaty fotograficzne i skanery	✓	–	–	–	–
---------------------------------	---	---	---	---	---

Reguły dostępu do urządzeń mobilnych




Urządzenia mobilne działające pod kontrolą systemu operacyjnego Android lub iOS są dzielone na kategorie jako urządzenia przenośne (MTP). Jeśli urządzenie mobilne jest podłączone do komputera, system operacyjny określa typ urządzenia. Jeśli na komputerze są zainstalowane aplikacje Android Debug Bridge (ADB), iTunes lub ich odpowiedniki, system operacyjny identyfikuje urządzenia mobilne jako urządzenia ADB lub iTunes. We wszystkich pozostałych przypadkach system operacyjny może zidentyfikować typ urządzenia mobilnego jako urządzenie przenośne (MTP) dla transferu plików, urządzenie PTP (kamera) dla transferu obrazów lub inne urządzenie. Typ urządzenia zależy od modelu urządzenia mobilnego.

Należy mieć na uwadze następujące kwestie specjalne związane z dostępem do urządzeń ADB lub iTunes:



- Nie możesz skonfigurować terminarza dostępu do urządzeń. Jeśli dostęp do urządzeń jest ograniczony przez reguły (posiadają stan ) , urządzenia ADB i iTunes nie zawsze są dostępne.
- Nie możesz skonfigurować dostępu do urządzenia dla pojedynczych użytkowników ani też skonfigurować uprawnień dostępu (odczyt/zapis). Jeśli dostęp do urządzeń jest ograniczony przez reguły (posiadają stan ) , urządzenia ADB i iTunes są dostępne dla wszystkich użytkowników ze wszystkimi uprawnieniami.
- Nie możesz skonfigurować dostępu do zaufanych urządzeń ADB lub iTunes dla pojedynczych użytkowników. Jeśli urządzenie jest zaufane, urządzenia ADB i iTunes są dostępne dla wszystkich użytkowników.
- Jeśli zainstalowałeś aplikacje ADB lub iTunes po podłączeniu urządzenia do komputera, unikatowy identyfikator urządzenia może zostać zresetowany. Oznacza to, że Kaspersky Endpoint Security zidentyfikuje to urządzenie jako nowe urządzenie. Jeśli urządzenie jest zaufane, ponownie dodaj urządzenie do listy zaufanych.

Domyślnie, reguły dostępu nadają wszystkim użytkownikom pełne prawa dostępu do urządzeń przez cały czas, jeżeli dozwolony jest dostęp do magistral połączeń odpowiednich typów urządzeń (stan ) .

Reguły dostępu dla sieci Wi-Fi

Reguła dostępu do sieci Wi-Fi określa, czy użycie sieci Wi-Fi jest dozwolone (stan ) lub zabronione (stan ) . Możesz dodać *zaufaną sieć Wi-Fi* (stan ) do reguły. Użycie zaufanej sieci Wi-Fi jest dozwolone bez ograniczeń. Domyślnie, reguła dostępu do sieci Wi-Fi zezwala na dostęp do dowolnej sieci Wi-Fi.


Reguły dostępu do magistrali połączeń

Reguły dostępu do magistrali połączeń określają, czy podłączenie urządzeń jest dozwolone (stan ) lub zabronione (stan ) . Reguły zezwalające na dostęp do magistral domyślnie są tworzone dla wszystkich magistral połączeń, które znajdują się w klasyfikacji modułu Kontrola urządzeń.

Modyfikowanie reguły dostępu do urządzenia

Reguła dostępu do urządzenia to grupa ustawień, które określają, którzy użytkownicy mogą uzyskać dostęp do urządzeń zainstalowanych na lub podłączonych do komputera. Te ustawienia obejmują dostęp do określonego urządzenia, dostęp do terminarza oraz uprawnienia odczytu i zapisu.

W celu zmodyfikowania reguły dostępu do urządzenia:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Urządzenia i sieci Wi-Fi**.

Otwarte okno wyświetla reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.

4. W sekcji **Dostęp do urządzeń magazynujących** wybierz regułę dostępu, którą chcesz edytować. Sekcja zawiera urządzenia z systemem plików, dla którego możesz skonfigurować dodatkowe ustawienia dostępu. Domyślnie reguła dostępu dla urządzenia nadaje wszystkim użytkownikom pełny dostęp do określonego typu urządzeń w dowolnym momencie.

a. W sekcji **Dostęp** wybierz odpowiednią opcję dostępu do urządzenia:

- **Zezwól.**
- **Blokuj.**
- **W zależności od połączenia magistrali.**

Aby zablokować lub zezwolić na dostęp do urządzenia, [skonfiguruj dostęp do magistrali połączeń](#).

- **Ogranicz zgodnie z regułami.**

Ta opcja umożliwia skonfigurowanie praw użytkownika, uprawnień i terminarza dla dostępu do urządzenia.

b. W oknie **Uprawnienia użytkowników** kliknij przycisk **Dodaj**.

Spowoduje to otwarcie okna dodania nowej reguły dostępu do urządzenia.

c. Przypisz priorytet do *reguły*. Reguła zawiera następujące atrybuty: konto użytkownika, terminarz, uprawnienia (odczyt/zapis) i priorytet.

Reguła posiada określony priorytet. Jeśli użytkownik został dodany do kilku grup, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o regułę z najwyższym priorytetem. Kaspersky Endpoint Security umożliwia przypisanie priorytetu od 0 do 10 000. Im większa wartość, tym większy priorytet. Innymi słowy, wpis z wartością 0 posiada najniższy priorytet.

Na przykład, możesz nadać uprawnienia tylko do odczytu grupie Każdy oraz nadać uprawnienia do odczytu/zapisu grupie administracyjnej. Aby to zrobić, przypisz priorytet 1 dla grupy administratorów oraz przypisz priorytet 0 dla grupy Każdy.

Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Innymi słowy, jeśli użytkownik został dodany do kilku grup, a priorytet wszystkich reguł jest taki sam, Kaspersky Endpoint Security reguluje dostęp urządzenia w oparciu o dowolną istniejącą regułę blokowania.

d. Ustaw stan **Włączony** dla reguły dostępu do urządzenia.

e. Skonfiguruj uprawnienia dostępu do urządzenia użytkowników: odczyt i/lub zapis.


f. Wybierz użytkowników lub grupy użytkowników, do których chcesz zastosować regułę dostępu do urządzenia.

g. Skonfiguruj terminarz dostępu do urządzenia dla użytkowników.

- h. Kliknij przycisk **Dodaj**.
5. W sekcji **Dostęp do urządzeń zewnętrznych** wybierz regułę i skonfiguruj dostęp: **Zezwól**, **Odmów** lub **W zależności od połączeń magistrali**. Jeśli to konieczne, [skonfiguruj dostęp do magistrali połączeń](#).
6. W sekcji **Dostęp do sieci Wi-Fi** kliknij odnośnik **Wi-Fi** i skonfiguruj dostęp: **Zezwól**, **Zablokuj** lub **Blokuj z wyjątkami**. Jeśli to konieczne, [dodaj sieci Wi-Fi do listy zaufanych](#).
7. Zapisz swoje zmiany.

Modyfikowanie reguły dostępu do magistrali połączeń


W celu zmodyfikowania reguły dostępu do magistrali połączeń:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij **Magistrale połączeń**.
Otwarte okno wyświetla reguły dostępu dla wszystkich magistral połączeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.
4. Wybierz regułę dostępu, którą chcesz zmienić.
5. W kolumnie **Dostęp** wybierz, czy chcesz zezwolić na dostęp do magistrali połączeń: **Zezwól** lub **Odmów**.
6. Zapisz swoje zmiany.

Dodawanie sieci Wi-Fi do listy zaufanych

Możesz zezwolić użytkownikom na łączenie się z sieciami Wi-Fi, które uważasz za bezpieczne, na przykład firmowa sieć Wi-Fi. W tym celu należy dodać sieć do listy zaufanych sieci Wi-Fi. Kontrola urządzeń zablokuje dostęp do wszystkich sieci Wi-Fi, za wyjątkiem tych określonych na liście zaufanych.

W celu dodania sieci Wi-Fi do listy zaufanych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Urządzenia i sieci Wi-Fi**.
Otwarte okno wyświetla reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.
4. W sekcji **Dostęp do sieci Wi-Fi** kliknij odnośnik **Wi-Fi**.
W otwartym oknie zostaną wyświetlone reguły dostępu do sieci Wi-Fi.
5. W kolumnie **Dostęp** wybierz **Blokuj z wyjątkami**.
6. W sekcji **Zaufane sieci Wi-Fi** kliknij **Dodaj**.

7. W otwartym oknie wykonaj jedną z następujących czynności:

- a. W polu **Nazwa sieci** określ nazwę sieci Wi-Fi, którą chcesz dodać do listy zaufanych.
- b. Z listy rozwijalnej **Typ autoryzacji** wybierz typ autoryzacji używanej podczas nawiązywania połączenia z zaufaną siecią Wi-Fi.
- c. Z listy rozwijalnej **Typ szyfrowania** wybierz rodzaj szyfrowania używanego podczas zabezpieczania ruchu zaufanej sieci Wi-Fi.
- d. W polu **Komentarz** możesz określić dowolne informacje o dodawanej sieci Wi-Fi.

Sieć Wi-Fi jest uznawana za zaufaną, jeśli jej ustawienia odpowiadają wszystkim ustawieniom określonym w regule.

8. Zapisz swoje zmiany.


Monitorowanie korzystania z nośników wymiennych

Monitorowanie korzystania z dysków wymiennych obejmuje:

- Monitorowanie działań wykonywanych na plikach na dyskach wymiennych.
- Monitorowanie podłączenia i odłączenia zaufanych dysków wymiennych.

Kaspersky Endpoint Security umożliwia monitorowanie podłączenia i odłączenia wszystkich zaufanych urządzeń, a nie tylko dysków wymiennych. Możesz włączyć zapisywanie zdarzeń w [ustawieniach powiadomień](#) dla komponentu Kontrola urządzeń. Zdarzenia posiadają priorytet *Zdarzenia informacyjne*.

W celu włączenia monitorowania korzystania z nośnika wymiennego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij przycisk **Urządzenia i sieci Wi-Fi**.
Otwarte okno wyświetla reguły dostępu dla wszystkich urządzeń, które znajdują się w klasyfikacji komponentu Kontrola urządzeń.
4. W sekcji **Dostęp do urządzeń magazynujących** wybierz **Dyski wymienne**.
5. Kliknij odnośnik **Logowanie**.
6. W otwartym oknie wybierz zakładkę **Logowanie**.
7. Włącz przełącznik **Logowanie**.
8. W sekcji **Operacje na plikach** wybierz operacje, które chcesz monitorować: **Zapis**, **Usuwanie**.
9. W sekcji **Filtruj według formatów plików** wybierz formaty plików, których skojarzone operacje powinny zostać zarejestrowane przez Kontrolę urządzeń.

10. Wybierz użytkowników lub grupy użytkowników korzystających z nośników wymiennych, które chcesz monitorować.

11. Zapisz swoje zmiany.

W wyniku tego działania, jeśli użytkownicy zapisują do plików znajdujących się na nośnikach wymiennych lub usuwają pliki z nośników wymiennych, Kaspersky Endpoint Security będzie zapisywał informacje o tych działaniach do raportu zdarzeń i wyśle zdarzenia do Kaspersky Security Center. Możesz wyświetlić zdarzenia skojarzone z plikami na nośnikach wymiennych w Konsoli administracyjnej Kaspersky Security Center, w obszarze roboczym węzła **Serwer administracyjny**, na zakładce **Zdarzenia**. Aby zdarzenia były wyświetlane w lokalnym raporcie zdarzeń Kaspersky Endpoint Security, w [ustawieniach powiadomień](#) modułu Kontrola urządzeń należy zaznaczyć pole **Operacja na pliku została wykonana**.

Zmiana czasu trwania buforowania

Komponent Kontrola urządzeń rejestruje zdarzenia dotyczące monitorowanych urządzeń, takie jak podłączanie i odłączanie urządzenia, odczyt pliku z urządzenia, zapis pliku na urządzeniu oraz inne zdarzenia. Następnie Kontrola urządzeń zezwala na lub blokuje działanie zgodnie z ustawieniami Kaspersky Endpoint Security.

Kontrola urządzeń zapisuje informacje o zdarzeniach dla określonego przedziału czasu zwanego *okresem buforowania*. Jeśli informacje dotyczące zdarzenia są buforowane, a to zdarzenie jest powtarzane, wówczas nie ma potrzeby informowania Kaspersky Endpoint Security o tym fakcie ani wyświetlać żadnego monitu o udzielenie dostępu do odpowiedniego działania, takiego jak nawiązanie połączenia z urządzeniem. To umożliwia wygodniejszą pracę z urządzeniem.

Zdarzenie jest uznawane za duplikat urządzenia, jeśli wszystkie następujące ustawienia zdarzenia odpowiadają wpisowi w pamięci podręcznej:

- ID urządzenia
- SID próby dostępu do konta użytkownika
- Kategoria urządzenia
- Działanie podjęte na urządzeniu
- Werdykt uprawnienia aplikacji dla tego działania: dozwolone lub zablokowane
- Ścieżka dostępu do procesu użytego do podjęcia działania
- Plik, do którego jest uzyskiwany dostęp

Przed zmianą okresu buforowania [wyłącz autoochronę Kaspersky Endpoint Security](#). Po zmianie okresu buforowania włącz autoochronę.

W celu zmiany okresu buforowania:

1. Otwórz edytor rejestru na komputerze.
2. W edytorze rejestru przejdź do następującej sekcji:
 - Dla 64-bitowych systemów operacyjnych:
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]

- Dla 32-bitowych systemów operacyjnych:
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]

3. Otwórz `DeviceControlEventsCachePeriod` do edycji.

4. Określ, przez ile minut Kontrola urządzeń musi zapisywać informacje o zdarzeniu zanim te informacje zostaną usunięte.

Działania podejmowane na zaufanych urządzeniach

Zaufane urządzenia są urządzeniami, do których użytkownicy, określani w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

Aby pracować z zaufanymi urządzeniami, możesz przyznać dostęp do pojedynczego użytkownika, grupy użytkowników lub wszystkich użytkowników organizacji.

Na przykład, jeśli Twoja organizacja nie zezwala na korzystanie z dysków wymiennych, ale administratorzy używają dysków wymiennych w swojej pracy, możesz zezwolić na dyski wymienne tylko dla grupy administratorów. Aby to zrobić, dodaj dyski wymienne do listy zaufanych i skonfiguruj uprawnienia dostępu użytkownika.

Kaspersky Endpoint Security pozwala dodać urządzenie do listy zaufanych w następujący sposób:

- Jeśli Kaspersky Security Center nie jest wdrożony w Twojej organizacji, możesz podłączyć urządzenie do komputera i [dodać je do listy zaufanych w ustawieniach aplikacji](#). Aby rozpowszechnić listę zaufanych urządzeń na wszystkich komputerach w organizacji, możesz włączyć scalanie list zaufanych urządzeń w zasadzie lub skorzystać z [procedury eksportu/importu](#).
- Jeśli Kaspersky Security Center jest wdrożony w Twojej organizacji, możesz zdalnie wykrywać wszystkie podłączone urządzenia i [utworzyć listę zaufanych urządzeń w zasadzie](#). Lista zaufanych urządzeń będzie dostępna na wszystkich komputerach, do których zastosowano zasadę.

Kaspersky Endpoint Security umożliwia kontrolowanie użycia zaufanych urządzeń (połączenie i rozłączenie). Możesz włączyć zapisywanie zdarzeń w [ustawieniach powiadomień](#) dla komponentu Kontrola urządzeń. Zdarzenia posiadają priorytet *Informacyjne*.


Podczas pracy z zaufanymi urządzeniami program Kaspersky Endpoint Security posiada następujące ograniczenia:

- Wtyczki administracyjne programu Kaspersky Endpoint Security w wersjach 11.0.0–11.2.0 nie mogą działać z listą zaufanych urządzeń, które zostały utworzone w Kaspersky Endpoint Security w wersji 11.3.0 i 11.4.0. Aby pracować z listą zaufanych urządzeń z tych wersji, wtyczka administracyjna musi zostać zaktualizowana do wersji 11.3.0 i 11.4.0.
- Wtyczki administracyjne programu Kaspersky Endpoint Security w wersjach 11.3.0 i 11.4.0 nie mogą działać z listą zaufanych urządzeń, które zostały utworzone w Kaspersky Endpoint Security w wersji 11.2.0 lub wcześniej. Aby te wersje działały z listą zaufanych urządzeń, aplikacja musi zostać zaktualizowana do wersji 11.3.0 i 11.4.0. Możesz także wysłać zgłoszenie zawierające opis sytuacji do pomocy technicznej za pośrednictwem [Kaspersky CompanyAccount](#).
- Aby przenieść listę zaufanych urządzeń z Kaspersky Endpoint Security w wersji 11.2.0 do wersji 11.3.0, wyślij zgłoszenie zawierające opis sytuacji do pomocy technicznej za pośrednictwem [Kaspersky CompanyAccount](#).

Dodawanie urządzenia do listy Zaufane z poziomu interfejsu aplikacji

Domyślnie podczas dodawania urządzenia do listy zaufanych urządzeń dostęp do niego jest dozwolony dla wszystkich użytkowników (grupa użytkowników Wszyscy).

W celu dodania urządzenia do listy Zaufane z poziomu interfejsu aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij **Zaufane urządzenia**.
Spowoduje to otwarcie listy zaufanych urządzeń.
4. Kliknij przycisk **Wybierz**.
Spowoduje to otwarcie listy podłączonych urządzeń. Lista urządzeń zależy od wartości wybranej z listy rozwijalnej **Wyświetl podłączone urządzenia**.
5. Na liście urządzeń wybierz urządzenie, które chcesz dodać do listy zaufanych.
6. W polu **Komentarz** możesz wprowadzić dowolne odpowiednie informacje o zaufanym urządzeniu.
7. Wybierz użytkowników lub grupy użytkowników, dla których chcesz zezwolić na dostęp do zaufanych urządzeń.
8. Zapisz swoje zmiany.

Dodawanie urządzenia do listy Zaufane z poziomu Kaspersky Security Center

Kaspersky Security Center otrzymuje informacje o urządzeniach, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerach i [włączona jest Kontrola urządzeń](#). Nie można dodać urządzenia do listy zaufanych, chyba że informacje o tym urządzeniu są dostępne w Kaspersky Security Center.

Możesz dodać urządzenie do listy zaufanych zgodnie z następującymi danymi:

- **Urządzenia według ID.** Każde urządzenie posiada unikatowy identyfikator (identyfikator sprzętu lub HWID). Możesz sprawdzić identyfikator we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Przykładowy identyfikator urządzenia: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Dodawanie urządzeń według identyfikatora jest wygodne, jeśli chcesz dodać kilka określonych urządzeń.
- **Urządzenia według modelu.** Każde urządzenie posiada identyfikator producenta (VID) oraz identyfikator produktu (PID). Możesz sprawdzić identyfikatory we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Szablon do wprowadzenia VID i PID: `VID_1234&PID_5678`. Dodawanie urządzeń według modelu jest wygodne, jeśli w swojej organizacji używasz urządzeń pewnego modelu. W ten sposób możesz dodać wszystkie urządzenia tego modelu.
- **Urządzenia według maski ID.** Jeśli używasz kilku urządzeń z podobnymi identyfikatorami, możesz dodać urządzenia do listy zaufanych, korzystając z maski. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład: `WDC_C*`.
- **Urządzenia według maski modelu.** Jeśli używasz kilku urządzeń z podobnymi numerami VID lub PID (na przykład, urządzeń od tego samego producenta), możesz dodać urządzenia do listy zaufanych przy użyciu masek. Znak `*` zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku `?` podczas wprowadzania maski. Na przykład: `VID_05AC & PID_*`.

W celu dodania urządzeń do listy zaufanych urządzeń:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
6. W prawej części okna wybierz zakładkę **Zaufane urządzenia**.
7. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę zaufanych urządzeń dla wszystkich komputerów w firmie.

Listy zaufanych urządzeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Zaufane urządzenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie zaufanych urządzeń zasady nadrzędnej nie jest możliwe.
8. Kliknij przycisk **Dodaj** i wybierz metodę dodawania urządzenia do listy zaufanych.
9. Aby filtrować urządzenia, wybierz typ urządzenia z listy rozwijanej **Typ urządzenia** (na przykład: **Dyski wymienne**).
10. W polu **Nazwa/model** wprowadź identyfikator urządzenia, model (identyfikator VID i identyfikator PID) lub maskę, w zależności od wybranej metody dodawania.

Dodawanie urządzeń według maski modelu (VID i PID) działa w następujący sposób: jeśli wprowadzisz maskę modelu, która nie odpowiada żadnemu modelowi, Kaspersky Endpoint Security sprawdza, czy identyfikator urządzenia (HWID) odpowiada masce. Kaspersky Endpoint Security sprawdza tylko część identyfikatora urządzenia, która określa producenta i typ urządzenia (SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000). Jeśli maska modelu odpowiada tej części identyfikatora urządzenia, urządzenia, które odpowiadają masce, zostaną dodane do listy zaufanych urządzeń na komputerze. W tym samym czasie lista urządzeń w Kaspersky Security Center pozostanie pusta po kliknięciu przycisku **Odśwież**. Aby poprawnie wyświetlić listę urządzeń, możesz dodać urządzenia według maski identyfikatora urządzenia.

11. Aby filtrować urządzenia, w polu **Komputer** wprowadź nazwę komputera lub maskę odpowiadającą nazwie komputera, do którego urządzenie jest podłączone.

Znak ***** zastępuje dowolny zestaw znaków. Znak **?** zastępuje dowolny pojedynczy znak.
12. Kliknij przycisk **Odśwież**.

Tabela wyświetla listę urządzeń, które spełniają zdefiniowane kryteria filtrowania.
13. Zaznacz pole obok nazw urządzeń, które chcesz dodać do listy zaufanych.
14. W polu **Komentarz** wprowadź opis przyczyny dodania urządzeń do listy zaufanych.
15. Kliknij przycisk **Wybierz** po prawej stronie pola **Zezwól użytkownikom i / lub grupom użytkowników**.
16. Wybierz użytkownika lub grupę w Active Directory i potwierdź swój wybór.

Domyślnie dostęp do zaufanych urządzeń jest dozwolony dla grupy Wszyscy.

17. Zapisz swoje zmiany.

Po podłączeniu urządzenia Kaspersky Endpoint Security sprawdza listę zaufanych urządzeń w poszukiwaniu autoryzowanego użytkownika. Jeśli urządzenie jest zaufane, Kaspersky Endpoint Security zezwala na dostęp do urządzenia ze wszystkimi uprawnieniami, nawet jeśli odmówiono dostępu do typu urządzenia lub magistrali połączenia. Jeśli urządzenie jest niezaufane, a dostęp jest zabroniony, możesz [poprosić o dostęp do zablokowanego urządzenia](#).


Eksportowanie i importowanie listy zaufanych urządzeń

Aby rozpowszechnić listę zaufanych urządzeń na wszystkich komputerach w organizacji, możesz skorzystać z procedury eksportu/importu.

Na przykład, jeśli chcesz rozpowszechnić listę zaufanych dysków wymiennych, wykonaj następujące czynności:

1. Podłącz kolejno dyski wymienne do komputera.
2. W ustawieniach Kaspersky Endpoint Security [dodaj dyski wymienne do listy zaufanych](#). W razie potrzeby skonfiguruj uprawnienia dostępu użytkownika. Na przykład, zezwalaj tylko administratorom na dostęp do dysków wymiennych.
3. Wyeksportuj listę zaufanych urządzeń w ustawieniach Kaspersky Endpoint Security (patrz instrukcje poniżej).
4. Prześlij plik listy zaufanych urządzeń na inne komputery w organizacji. Na przykład, umieść plik w folderze udostępnionym.
5. Zaimportuj listę zaufanych urządzeń w ustawieniach Kaspersky Endpoint Security na inne komputery w organizacji (patrz instrukcje poniżej).

W celu zaimportowania lub wyeksportowania listy zaufanych urządzeń:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij **Zaufane urządzenia**.
Spowoduje to otwarcie listy zaufanych urządzeń.
4. W celu wyeksportowania listy zaufanych urządzeń:
 - a. Wybierz zaufane urządzenia, które chcesz wyeksportować.
 - b. Kliknij przycisk **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę zaufanych urządzeń, wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje całą listę zaufanych urządzeń do pliku XML.
5. W celu zaimportowania listy zaufanych urządzeń:

a. Z listy rozwijalnej **Importuj** wybierz odpowiednie działanie: **Importuj i dodaj do istniejących** lub **Importuj i zastąp istniejące**.

b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę zaufanych urządzeń.

c. Kliknij przycisk **Otwórz**.

Jeśli komputer ma już listę zaufanych urządzeń, Kaspersky Endpoint Security wyświetli monit o usunięciu istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

6. Zapisz swoje zmiany.

Po podłączeniu urządzenia Kaspersky Endpoint Security sprawdza listę zaufanych urządzeń w poszukiwaniu autoryzowanego użytkownika. Jeśli urządzenie jest zaufane, Kaspersky Endpoint Security zezwala na dostęp do urządzenia ze wszystkimi uprawnieniami, nawet jeśli odmówiono dostępu do typu urządzenia lub magistrali połączenia.

Uzyskiwanie dostępu do zablokowanego urządzenia

Podczas konfigurowania Kontroli urządzeń możesz przez przypadek zablokować dostęp do urządzenia, które jest potrzebne do pracy.

Jeśli Kaspersky Security Center nie jest zainstalowany w Twojej organizacji, możesz udzielić dostępu do urządzenia w ustawieniach Kaspersky Endpoint Security. Na przykład, możesz [dodać urządzenie do listy zaufanych](#) lub tymczasowo [wyłączyć Kontrolę urządzeń](#).

Jeśli Kaspersky Security Center jest zainstalowany w Twojej organizacji, a profil został zastosowany do komputerów, możesz zapewnić dostęp do urządzenia w Konsoli administracyjnej.

Tryb online dla zezwalania na dostęp

Możesz zezwolić na dostęp do zablokowanego urządzenia w trybie online tylko wtedy, gdy Kaspersky Security Center jest zainstalowany w organizacji, a profil został zastosowany do komputera. Komputer musi mieć możliwość nawiązania połączenia z Serwerem administracyjnym.

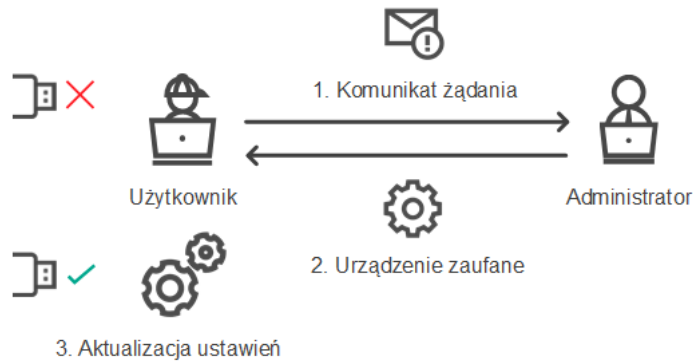
Zezwalanie na dostęp w trybie online obejmuje następujące kroki:

1. Użytkownik wysłał do administratora wiadomość zawierającą żądanie dostępu.

2. Administrator dodaje urządzenie do listy zaufanych.

Możesz dodać zaufane urządzenie w profilu dla grupy administracyjnej lub w lokalnych ustawieniach aplikacji dla pojedynczego komputera.

3. Administrator aktualizuje ustawienia Kaspersky Endpoint Security na komputerze użytkownika.



Schemat zezwalania na dostęp do urządzenia w trybie online

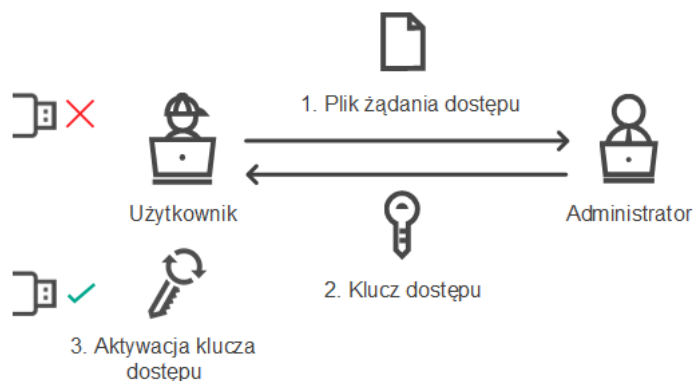
Tryb offline dla zezwalania na dostęp

Możesz zezwolić na dostęp do zablokowanego urządzenia w trybie offline tylko wtedy, gdy Kaspersky Security Center jest zainstalowany w organizacji, a profil został zastosowany do komputera. W ustawieniach profilu, w sekcji **Kontrola urządzeń**, pole **Zezwól na żądania dostępu tymczasowego** musi zostać zaznaczone.

Jeśli konieczne jest zezwolenie na dostęp tymczasowy do zablokowanego urządzenia, ale nie możesz [dodać urządzenia do listy zaufanych](#), możesz zezwolić na dostęp do urządzenia w trybie offline. W ten sposób możesz zezwolić na dostęp do zablokowanego urządzenia nawet wtedy, gdy komputer nie ma dostępu do sieci lub jeśli komputer znajduje się poza siecią firmową.

Zezwalanie na dostęp w trybie offline obejmuje następujące kroki:

1. Użytkownik utworzy plik zawierający żądanie dostępu i wyśle go do administratora.
2. Administrator utworzy klucz dostępu z pliku zawierającego żądanie dostępu i wyśle go do użytkownika.
3. Użytkownik aktywuje klucz dostępu.



Schemat zezwalania na dostęp do urządzenia w trybie offline

Tryb online dla zezwalania na dostęp

Możesz zezwolić na dostęp do zablokowanego urządzenia w trybie online tylko wtedy, gdy Kaspersky Security Center jest zainstalowany w organizacji, a profil został zastosowany do komputera. Komputer musi mieć możliwość nawiązania połączenia z Serwerem administracyjnym.

Użytkownik żąda dostępu do zablokowanego urządzenia w następujący sposób:

1. Podłącz urządzenie do komputera.

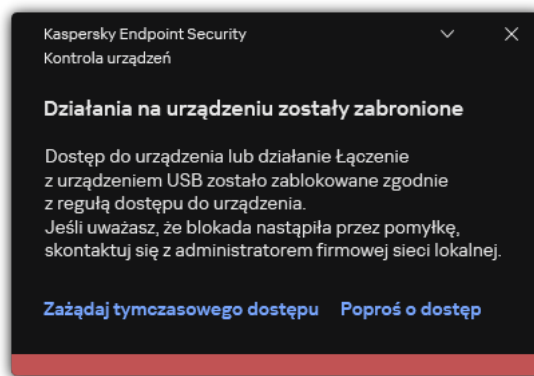
Kaspersky Endpoint Security wyświetli powiadomienie informujące, że dostęp do urządzenia zostanie zablokowany (patrz rysunek poniżej).

2. Kliknij **Żądanie dostępu**.

To spowoduje otwarcie okna **Wiadomość do administratora**. Ta wiadomość zawiera informacje o zablokowanym urządzeniu.

3. Kliknij przycisk **Wyślij**.

Administrator otrzyma wiadomość zawierającą żądanie dostępu, na przykład, za pośrednictwem poczty elektronicznej. Więcej informacji o przetwarzaniu żądań użytkowników można znaleźć w [pomocy do Kaspersky Security Center](#). Po [dodaniu urządzenia do listy zaufanych](#) i zaktualizowaniu ustawień Kaspersky Endpoint Security na komputerze, użytkownik uzyska dostęp do urządzenia.



Komunikat Kontroli urządzeń

Tryb offline dla zezwalania na dostęp

Możesz zezwolić na dostęp do zablokowanego urządzenia w trybie offline tylko wtedy, gdy Kaspersky Security Center jest zainstalowany w organizacji, a profil został zastosowany do komputera. W ustawieniach profilu, w sekcji **Kontrola urządzeń**, pole **Zezwól na żądanie tymczasowego dostępu** musi zostać zaznaczone.

Użytkownik żąda dostępu do zablokowanego urządzenia w następujący sposób:

1. Podłącz urządzenie do komputera.

Kaspersky Endpoint Security wyświetli powiadomienie informujące, że dostęp do urządzenia zostanie zablokowany (patrz rysunek poniżej).

2. Kliknij odnośnik **Zażądaj tymczasowego dostępu**.

Zostanie otwarte okno zawierające listę podłączonych urządzeń.

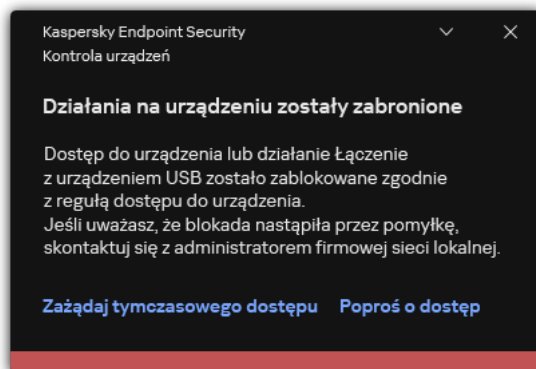
3. Z listy podłączonych urządzeń wybierz urządzenie, do którego chcesz uzyskać dostęp.

4. Kliknij **Uzyskaj plik żądania dostępu**.

5. W polu **Czas dostępu** określ przedział czasu, podczas którego chcesz mieć dostęp do urządzenia.

6. Zapisz plik w pamięci komputera.

W rezultacie plik z żądaniem dostępu z rozszerzeniem *.akey zostanie pobrany do pamięci komputera. Użyj dowolnej dostępnej metody wysyłania pliku z żądaniem dostępu do urządzenia do administratora korporacyjnej sieci LAN.



Komunikat Kontroli urządzeń

[Jak administrator może utworzyć klucz dostępu do zablokowanego urządzenia w Konsoli administracyjnej \(MMC\) [?]](#)


1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder z nazwą grupy administracyjnej, do której należy wybrany komputer kliencki.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Na liście komputerów klienckich wybierz komputer, którego użytkownik ma uzyskać tymczasowy dostęp do zablokowanego urządzenia.
5. Z menu kontekstowego komputera wybierz element **Przydziel dostęp w trybie offline**.
6. W otwartym oknie wybierz zakładkę **Kontrola urządzeń**.
7. Kliknij przycisk **Przeglądaj** i pobierz plik zawierający żądanie dostępu, otrzymany od użytkownika.
Zostaną wyświetlone informacje o zablokowanym urządzeniu, do którego użytkownik zażądał dostępu.
8. Jeśli to konieczne, zmień wartość ustawienia **Czas dostępu**.
Domyślnie, ustawienie **Czas dostępu** przyjmuje wartość, która została wskazana przez użytkownika podczas tworzenia pliku żądania dostępu.
9. Określ wartość ustawienia **Aktywny przez**.
Ustawienie to definiuje przedział czasu, podczas którego użytkownik może aktywować dostęp do zablokowanego urządzenia przy pomocy klucza dostępu.
10. Zapisz plik klucza dostępu w pamięci komputera.

[Jak administrator może utworzyć klucz dostępu do zablokowanego urządzenia w Web Console i Cloud Console [?]](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Na liście komputerów klienckich wybierz komputer, którego użytkownik ma uzyskać tymczasowy dostęp do zablokowanego urządzenia.
3. Kliknij przycisk wielokropka () nad listą komputerów, a następnie kliknij przycisk **Przyznaj dostęp do urządzenia w trybie offline**.
4. W otwartym oknie wybierz sekcję **Kontrola urządzeń**.
5. Kliknij przycisk **Przełączaj** i pobierz plik zawierający żądanie dostępu, otrzymany od użytkownika.
Zostaną wyświetlone informacje o zablokowanym urządzeniu, do którego użytkownik zażądał dostępu.
6. Jeśli to konieczne, zmień wartość ustawienia **Czas dostępu (godziny)**.
Domyślnie, ustawienie **Czas dostępu (godziny)** przyjmuje wartość, która została wskazana przez użytkownika podczas tworzenia pliku żądania dostępu.
7. Ustaw okres czasu, w którym klucz dostępu może być aktywowany na urządzeniu.
Ustawienie to definiuje przedział czasu, podczas którego użytkownik może aktywować dostęp do zablokowanego urządzenia przy pomocy klucza dostępu.
8. Zapisz plik klucza dostępu w pamięci komputera.

W rezultacie zablokowany klucz dostępu do urządzenia zostanie pobrany do pamięci komputera. Plik klucza dostępu posiada rozszerzenie *.acode. Użyj dowolnej dostępnej metody, aby wysłać klucz dostępu do zablokowanego urządzenia do użytkownika.

Użytkownik aktywuje klucz dostępu w następujący sposób:

1. W [oknie głównym aplikacji](#) kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Żądanie dostępu** kliknij przycisk **Żądanie dostępu do urządzenia**.
4. W otwartym oknie kliknij przycisk **Aktywuj klucz dostępu**.
5. W otwartym oknie wybierz plik z kluczem dostępu do urządzenia, otrzymany od administratora korporacyjnej sieci LAN.
Spowoduje to otwarcie okna zawierającego informacje o zapewnieniu dostępu.
6. Kliknij **OK**.


W rezultacie użytkownik uzyska dostęp do urządzenia na czas określony przez administratora. Użytkownik otrzyma pełny zestaw uprawnień dostępu do urządzenia (odczyt i zapis). Po wygaśnięciu klucza, dostęp do urządzenia zostanie zablokowany. Jeśli użytkownik żąda tymczasowego dostępu do urządzenia, [dodaj urządzenie do listy zaufanych](#).

Modyfikowanie szablonów wiadomości Kontroli urządzeń

Kiedy użytkownik próbuje uzyskać dostęp do zablokowanego urządzenia, Kaspersky Endpoint Security wyświetla wiadomość informującą, że dostęp do urządzenia jest zablokowany lub operacja na zawartości urządzenia jest zabroniona. Jeśli użytkownik uważa, że dostęp do urządzenia został zablokowany lub operacja na zawartości urządzenia jest zabroniona przez pomyłkę, może wysłać wiadomość do administratora lokalnej sieci firmowej poprzez kliknięcie odnośnika w wyświetlonej wiadomości.

Szablony są dostępne dla wiadomości dotyczących zablokowanego dostępu do urządzeń, niedozwolonych działań na zawartości urządzenia oraz wiadomości wysłanych do administratora. Możesz zmodyfikować szablony wiadomości.

W celu zmodyfikowania szablonów dla wiadomości Kontroli urządzeń:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Szablony wiadomości** skonfiguruj szablony dla wiadomości Kontroli urządzeń:
 - **Wiadomość dotycząca blokowania.** Szablon wiadomości, która pojawia się, gdy użytkownik próbuje uzyskać dostęp do zablokowanego urządzenia. Ta wiadomość pojawia się, gdy użytkownik próbuje wykonać działanie na zawartości urządzenia, które zostało zablokowane dla tego użytkownika.
 - **Wiadomość do administratora.** Szablon wiadomości, która jest wysyłana do administratora sieci LAN, gdy użytkownik uważa, że dostęp do urządzenia lub wykonywanie działań na zawartości urządzenia zostały zablokowane przez przypadek. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania dostępu do urządzenia** Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkowników**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.
4. Zapisz swoje zmiany.

Anti-Bridging

Anti-Bridging zapobiega tworzeniu mostków sieciowych poprzez uniemożliwienie jednoczesnego nawiązania kilku połączeń sieciowych dla komputera. To umożliwia ochronę sieci firmowej przed atakami na niechronione, nieautoryzowane sieci.

Anti-Bridging reguluje nawiązywanie połączeń sieciowych przy użyciu *reguł połączenia*.

Reguły połączenia są tworzone dla następujących predefiniowanych typów urządzeń:

- Karty sieciowe;
- Karty Wi-Fi;
- Modemy.

Jeśli reguła połączenia jest używana, Kaspersky Endpoint Security:


- Blokuje aktywne połączenie podczas nawiązywania nowego połączenia, jeśli typ urządzenia, określony w regule, jest używany dla obu połączeń;

- Blokuje nawiązane połączenia przy użyciu typów urządzeń, dla których używane są reguły o niższym priorytecie.

Włączanie modułu Anti-Bridging

Domyślnie moduł Anti-Bridging jest wyłączony.


W celu włączenia modułu Anti-Bridging:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij **Anti-Bridging**.
4. Użyj przełącznika **Włącz Anti-Bridging**, aby włączyć lub wyłączyć tę funkcję.
5. Zapisz swoje zmiany.

Po włączeniu modułu Anti-Bridging, Kaspersky Endpoint Security blokuje już nawiązane połączenia zgodnie z regułami połączeń.


Zmiana stanu reguły połączenia

W celu zmiany stanu reguły połączenia:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij **Anti-Bridging**.
4. W sekcji **Reguły dla urządzeń** wybierz regułę, której stan chcesz zmienić.
5. Użyj przełączników w kolumnie **Kontrola**, aby włączyć lub wyłączyć regułę.
6. Zapisz swoje zmiany.

Zmiana priorytetu reguły połączenia

W celu zmiany priorytetu reguły połączenia:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola urządzeń**.
3. W sekcji **Ustawienia dostępu** kliknij **Anti-Bridging**.
4. W sekcji **Reguły dla urządzeń** wybierz regułę, której priorytet chcesz zmienić.

5. Użyj przycisków **W górę** / **W dół**, aby ustawić priorytet reguły połączenia.

Im wyżej reguła znajduje się w tabeli reguł, tym wyższy priorytet posiada. Anti-Bridging blokuje wszystkie połączenia za wyjątkiem jednego połączenia nawiązanego przy użyciu typu urządzenia, dla którego używana jest reguła najwyższego poziomu.

6. Zapisz swoje zmiany.

Adaptacyjna kontrola anomalii

Ten komponent jest dostępny tylko dla Kaspersky Endpoint Security for Business Advanced i Kaspersky Total Security for Business. Więcej informacji o Kaspersky Endpoint Security for Business można znaleźć na [stronie internetowej firmy Kaspersky](#).

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Komponent Adaptacyjna kontrola anomalii monitoruje i blokuje działania, które nie są typowe dla komputerów w sieci firmowej. Adaptacyjna kontrola anomalii wykorzystuje zestaw reguł do śledzenia nietypowych zachowań (na przykład, reguła *Uruchom Microsoft PowerShell z aplikacji biurowych*). Reguły są tworzone przez specjalistów z Kaspersky w oparciu o typowe scenariusze złośliwej aktywności. Można skonfigurować, w jaki sposób Adaptacyjna kontrola aplikacji obsługuje każdą regułę i, na przykład, zezwolić na wykonywanie skryptów PowerShell, które automatyzują określone zadania przepływu pracy. Kaspersky Endpoint Security aktualizuje zestaw reguł wraz z bazami danych aplikacji. Aktualizacje zestawów reguł muszą być [potwierdzone ręcznie](#).

Ustawienia komponentu Adaptacyjna kontrola anomalii

Konfiguracja Adaptacyjnej kontroli anomalii składa się z następujących kroków:

1. Uczenie modułu Adaptacyjna kontrola anomalii.

Po włączeniu Adaptacyjnej kontroli anomalii, jej reguły działają w *trybie uczenia*. Podczas uczenia moduł Adaptacyjna kontrola anomalii monitoruje wyzwalanie reguł i wysyła zdarzenia wyzwalające do Kaspersky Security Center. Każda reguła ma swój czas trwania trybu uczenia. Czas trwania trybu uczenia jest ustawiany przez ekspertów z Kaspersky. Zazwyczaj tryb uczenia jest aktywny przez dwa tygodnie.

Jeśli podczas treningu reguła nie została w ogóle uruchomiona, Adaptacyjna kontrola anomalii uzna działania związane z tą regułą za nietypowe. Kaspersky Endpoint Security zablokuje wszystkie działania związane z tą regułą.

Jeśli reguła została wyzwolona podczas treningu, Kaspersky Endpoint Security rejestruje zdarzenia w [raporcie wyzwalającym regułę](#) oraz w repozytorium **Wywoływanie reguł w trybie Inteligentne uczenie**.

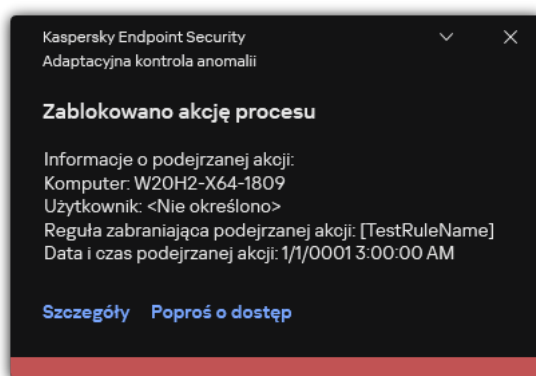
2. Analizowanie raportu dotyczącego wyzwalania reguły.

Administrator analizuje [raport dotyczący wyzwalania reguły](#), lub zawartość repozytorium **Wywoływanie reguł w trybie Inteligentne uczenie**. Następnie administrator może wybrać zachowanie Adaptacyjnej kontroli anomalii, gdy reguła jest wyzwalana: albo zablokować, albo zezwolić. Administrator może również kontynuować monitorowanie działania reguły i wydłużyć czas trwania trybu uczenia. Jeśli administrator nie podejmie żadnych działań, aplikacja będzie również kontynuować pracę w trybie uczenia. Czas trwania trybu uczenia zostanie zrestartowany.

Adaptacyjna kontrola anomalii jest konfigurowana w czasie rzeczywistym. Adaptacyjna kontrola anomalii jest konfigurowana poprzez następujące kanały:

- Adaptacyjna kontrola anomalii automatycznie rozpoczyna blokowanie działań związanych z regułami, które nigdy nie zostały wyzwolone w trybie uczenia.
- Kaspersky Endpoint Security dodaje nowe reguły lub usuwa przestarzałe.
- Administrator konfiguruje działanie Adaptacyjnej kontroli anomalii po przejrzaniu raportu dotyczącego wyzwalania reguły i zawartości repozytorium **Wyzwalanie reguł w trybie Inteligentne uczenie**. Zalecane jest sprawdzenie raportu dotyczącego wyzwalania reguły i zawartości repozytorium **Wyzwalanie reguł w trybie Inteligentne uczenie**.

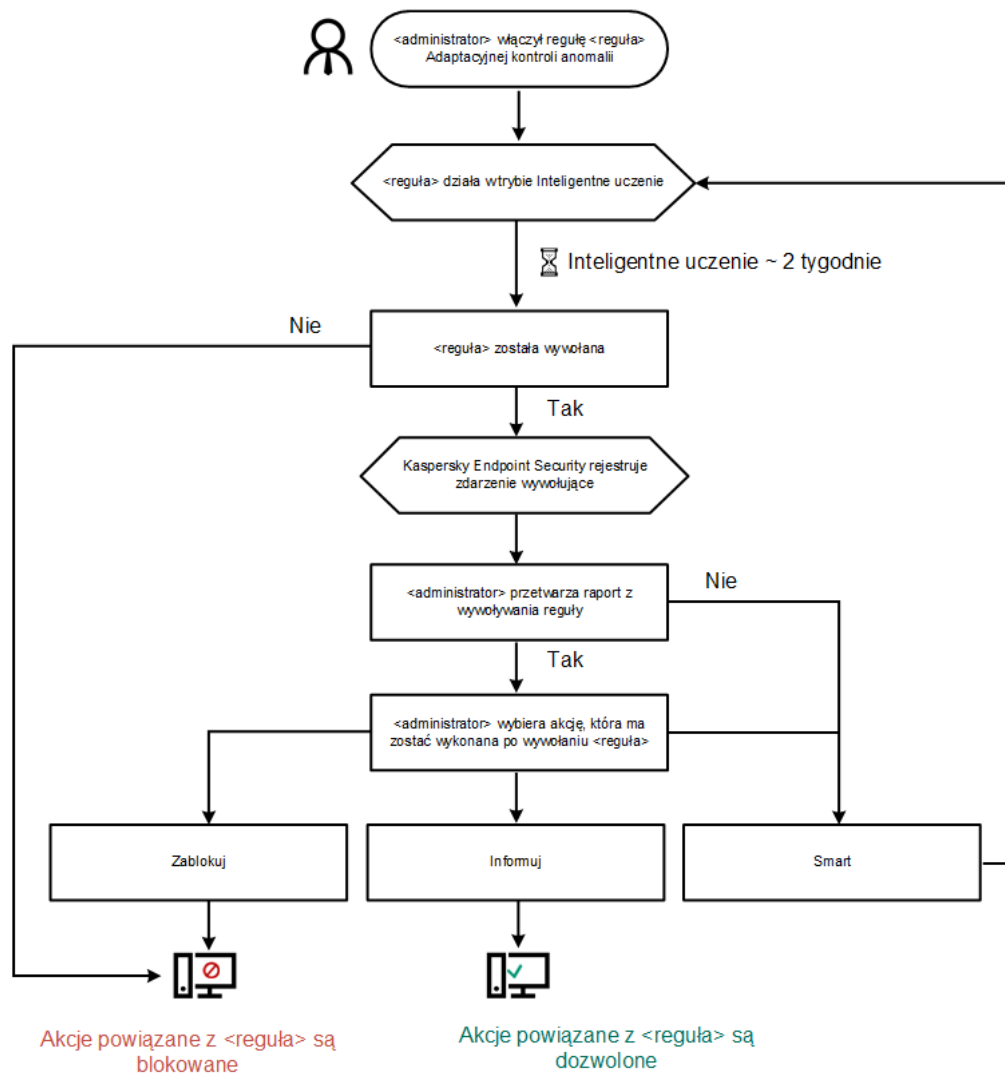
Jeśli złośliwa aplikacja spróbuje wykonać akcję, Kaspersky Endpoint Security zablokuje tę akcję i wyświetli powiadomienie (patrz rysunek poniżej).



Powiadomienie Adaptacyjnej kontroli anomalii

Algorytm działania Adaptacyjnej kontroli anomalii

Kaspersky Endpoint Security decyduje, czy zezwolić na lub zablokować działanie skojarzone z regułą opartą o następujący algorytm (patrz rysunek poniżej).




Algorytm działania Adaptacyjnej kontroli anomalii

Włączanie i wyłączanie Adaptacyjnej kontroli anomalii

Domyślnie, Adaptacyjna kontrola anomalii jest włączona.

W celu włączenia i wyłączenia Adaptacyjnej kontroli anomalii:


1. W [oknie głównym aplikacji](#) kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. Użyj przełącznika **Adaptacyjna kontrola anomalii**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

W rezultacie Adaptacyjna kontrola anomalii przełączy się w tryb uczenia. Podczas uczenia Adaptacyjna kontrola anomalii monitoruje uruchamianie reguł. Po zakończeniu uczenia Adaptacyjna kontrola anomalii zaczyna blokować działania, które nie są typowe dla komputerów w sieci firmowej.

Jeśli Twoja organizacja zaczęła używać nowych narzędzi, a Adaptacyjna kontrola anomalii blokuje działanie tych narzędzi, możesz zresetować wyniki trybu uczenia i powtórzyć uczenie. Aby to zrobić, musisz [zmienić akcję podejmowaną po wywołaniu reguły](#) (na przykład ustawić ją na **Powiadom**). Następnie należy ponownie włączyć tryb uczenia (ustawić wartość **Smart**).


Włączanie i wyłączanie reguły Adaptacyjnej kontroli anomalii

W celu włączenia lub wyłączenia reguły Adaptacyjnej kontroli anomalii:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.
Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.
4. W tabeli wybierz zestaw reguł (na przykład: *Aktywność aplikacji biurowych*) i rozwiń zestaw.
5. Wybierz regułę (na przykład: *Uruchom Windows PowerShell z aplikacji biurowych*).
6. Użyj przełącznika w kolumnie **Stan**, aby włączyć lub wyłączyć regułę Adaptacyjnej kontroli anomalii.
7. Zapisz swoje zmiany.

Modyfikowanie akcji podejmowanej w momencie wyzwolenia reguły Adaptacyjnej kontroli anomalii

W celu zmodyfikowania akcji podejmowanej w momencie wyzwolenia reguły Adaptacyjnej kontroli anomalii:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.
Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.
4. Wybierz regułę w tabeli.
5. Kliknij przycisk **Edytuj**.
Zostanie otwarte okno właściwości reguły Adaptacyjnej kontroli anomalii.
6. W sekcji **Akcja** wybierz jedną z następujących opcji:
 - **Smart**. Jeśli ta opcja jest zaznaczona, reguły Adaptacyjnej kontroli anomalii działa w trybie Inteligentne uczenie się przez czas zdefiniowany przez ekspertów z Kaspersky. W tym trybie, gdy reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zezwoli na aktywność objęta regułą i zarejestruje wpis w magazynie **Wywoływanie reguł w trybie Inteligentne uczenie** Serwera administracyjnego Kaspersky Security Center. Jeśli przedział czasu ustawiony dla trybu Inteligentne uczenie

się zostanie zakończony, Kaspersky Endpoint Security zablokuje aktywność objętą regułą Adaptacyjna kontrola anomalii i zarejestruje wpis zawierający informacje o aktywności.

- **Blokuj.** Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zablokuje aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.
- **Informuj.** Jeśli to działanie jest wybrane, reguła Adaptacyjnej kontroli anomalii zostanie wyzwolona, Kaspersky Endpoint Security zezwoli na aktywność objętą regułą i zarejestruje wpis zawierający informacje o aktywności.


7. Zapisz swoje zmiany.

Tworzenie wykluczeń dla reguły Adaptacyjnej kontroli anomalii

Nie możesz utworzyć więcej niż 1 000 wykluczeń dla reguł Adaptacyjnej kontroli anomalii. Nie jest zalecane tworzenie więcej niż 200 wykluczeń. Aby zmniejszyć liczbę używanych wykluczeń, zalecane jest używanie masek w ustawieniach wykluczeń.

Wykluczenie dla reguły Adaptacyjnej kontroli anomalii zawiera opis obiektów źródłowych i docelowych. *Obiekt źródłowy* to obiekt wykonujący działania. *Obiekt docelowy* to obiekt, na którym wykonywane są działania. Na przykład, otworzyłeś plik o nazwie `file.xlsx`. W rezultacie plik biblioteki z rozszerzeniem DLL jest załadowywany do pamięci komputera. Ta biblioteka jest używana przez przeglądarkę (plik wykonywalny o nazwie `browser.exe`). W tym przykładzie `file.xlsx` to obiekt źródłowy, Excel to proces źródłowy, `browser.exe` to obiekt docelowy, a Browser to proces docelowy.

W celu utworzenia wykluczenia dla reguły Adaptacyjnej kontroli anomalii:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.
Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.
4. Wybierz regułę w tabeli.
5. Kliknij przycisk **Edytuj**.
Zostanie otwarte okno właściwości reguły Adaptacyjnej kontroli anomalii.
6. W sekcji **Wykluczenia** kliknij przycisk **Dodaj**.
Zostanie otwarte okno właściwości wykluczenia.
7. Wybierz użytkownika, dla którego chcesz skonfigurować wykluczenie.

Adaptacyjna kontrola anomalii nie obsługuje wykluczeń dla grup użytkowników. Jeśli wybierzesz grupę użytkowników, Kaspersky Endpoint Security nie stosuje wykluczenia.

8. W polu **Opis** wprowadź opis wykluczenia.

9. Zdefiniuj ustawienia obiektu źródłowego lub procesu źródłowego uruchomionego przez obiekt:

- **Proces źródłowy.** Ścieżka lub maska ścieżki do pliku lub folderu zawierającego pliki (na przykład: C:\Dir\File.exe lub Dir*.exe).
- **Suma kontrolna procesu źródłowego.** Suma kontrolna pliku.
- **Obiekt źródłowy.** Ścieżka lub maska ścieżki do pliku lub folderu zawierającego pliki (na przykład: C:\Dir\File.exe lub Dir*.exe). Na przykład, ścieżka do pliku document.docm, która wykorzystuje skrypt lub makro do uruchamiania procesów docelowych.
Możesz także określić inne obiekty, które powinny zostać wykluczone, takie jak adres internetowy, makra, polecenie w wierszu polecenia, ścieżka do rejestru lub inne. Określ obiekt zgodnie z następującym szablonem: `object://<obiekt>`, gdzie <obiekt> odnosi się do nazwy obiektu, na przykład, `object://web.site.example.com`, `object://VBA`, `object://ipconfig`, `object://HKEY_USERS`. Można też użyć masek, na przykład, `object://*C:\Windows\temp*`.
- **Suma kontrolna obiektu źródłowego.** Suma kontrolna pliku.

Reguła Adaptacyjnej kontroli anomalii nie jest stosowana do działań wykonywanych przez obiekt lub do procesów uruchomionych przez obiekt.

10. Określ ustawienia obiektu docelowego lub procesów docelowych uruchomionych na obiekcie.


- **Proces docelowy.** Ścieżka lub maska ścieżki do pliku lub folderu zawierającego pliki (na przykład: C:\Dir\File.exe lub Dir*.exe).
- **Suma kontrolna procesu docelowego.** Suma kontrolna pliku.
- **Obiekt docelowy.** Polecenie uruchamiające proces docelowy. Określ polecenie, używając następującego wzoru `object://<polecenie>`, na przykład: `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`. Można też użyć masek, na przykład, `object://*C:\Windows\temp*`.
- **Suma kontrolna obiektu docelowego.** Suma kontrolna pliku.

Reguła Adaptacyjnej kontroli anomalii nie jest stosowana do działań podejmowanych na obiekcie lub do procesów uruchomionych na obiekcie.

11. Zapisz swoje zmiany.

Eksportowanie i importowanie wykluczeń dla reguł Adaptacyjnej kontroli anomalii

W celu wyeksportowania lub zaimportowania listy wykluczeń dla wybranych reguł:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.
Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.
4. W celu wyeksportowania listy reguł:


- a. Wybierz reguły, których wyjątki chcesz wyeksportować.
 - b. Kliknij przycisk **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Potwierdź chęć wyeksportowania tylko wybranych wykluczeń lub wyeksportuj całą listę wykluczeń.
 - e. Kliknij przycisk **Zapisz**.
5. W celu zaimportowania listy reguł:
- a. Kliknij przycisk **Importuj**.
 - b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.
 - c. Kliknij przycisk **Otwórz**.
- Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
6. Zapisz swoje zmiany.

Stosowanie aktualizacji dla reguł Adaptacyjnej kontroli anomalii

Nowe reguły Adaptacyjnej kontroli anomalii mogą zostać dodane do tabeli reguł, a istniejące reguły Adaptacyjnej kontroli anomalii mogą zostać usunięte z tabeli reguł po zaktualizowaniu antywirusowych baz danych. Kaspersky Endpoint Security rozróżnia reguły Adaptacyjnej kontroli anomalii, które mają zostać usunięte lub dodane do tabeli, jeśli aktualizacja dla tych reguł nie została zastosowana.

Dopóki aktualizacja nie zostanie zastosowana, Kaspersky Endpoint Security wyświetli reguły Adaptacyjnej kontroli anomalii ustawione do usunięcia przez aktualizację w tabeli reguł i przypisze do nich stan *Wyłączona*. Nie jest możliwa zmiana ustawień tych reguł.

W celu zastosowania aktualizacji dla reguł Adaptacyjnej kontroli anomalii:


1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Reguły** kliknij przycisk **Edytuj reguły**.
Zostanie otwarta lista Reguła Adaptacyjnej kontroli anomalii.
4. W otwartym oknie kliknij przycisk **Zatwierdź aktualizacje**.
Przycisk **Zatwierdź aktualizacje** jest dostępny, jeśli aktualizacja dla reguł Adaptacyjnej kontroli anomalii jest dostępna.
5. Zapisz swoje zmiany.

Modyfikowanie szablonów wiadomości Adaptacyjnej kontroli anomalii

Jeśli użytkownik spróbuje wykonać działanie zablokowane przez Adaptacyjną kontrolę anomalii, Kaspersky Endpoint Security wyświetli komunikat o zablokowaniu potencjalnie szkodliwych działań. Jeżeli użytkownik ma pewność, że działanie zostało zablokowane przez pomyłkę, powinien użyć odnośnika dostępnego w wiadomości w celu przesłania zgłoszenia do administratora lokalnej sieci firmowej.

Dostępne są specjalne szablony wiadomości o zablokowaniu potencjalnie szkodliwych działań oraz wiadomości wysyłanych do administratora. Możesz zmodyfikować szablony wiadomości.

W celu zmodyfikowania szablonu wiadomości:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
3. W sekcji **Szablony** skonfiguruj szablony dla wiadomości Adaptacyjnej kontroli anomalii:
 - **Wiadomość dotycząca blokowania.** Szablon komunikatu, który jest wyświetlany użytkownikowi po wyzwoleniu reguły komponentu Adaptacyjna kontrola anomalii, która blokuje nietypowe działanie.
 - **Wiadomość do administratora.** Szablon wiadomości dla użytkownika, która może zostać wysłana do lokalnego administratora sieci korporacyjnej, jeśli użytkownik uzna, że zablokowanie jest pomyłką. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania aktywności aplikacji** Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkowników**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.
4. Zapisz swoje zmiany.

Przeglądanie raportów Adaptacyjnej kontroli anomalii

W celu przejrzenia raportów Adaptacyjnej kontroli anomalii:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Adaptacyjna kontrola anomalii**.
Ustawienia modułu Adaptacyjna kontrola anomalii są wyświetlane w prawej części okna.
6. Wykonaj jedną z poniższych czynności:

- Jeśli chcesz przejrzeć raport dotyczący ustawień reguł Adaptacyjnej kontroli anomalii, kliknij **Raport o stanie reguł Adaptacyjnej kontroli anomalii**.
- Jeśli chcesz przejrzeć raport dotyczący wyzwalania reguł Adaptacyjnej kontroli anomalii, kliknij przycisk **Raport o wywołanych regułach Adaptacyjnej kontroli anomalii**.

7. Zostanie rozpoczęty proces tworzenia raportu.

Raport zostanie wyświetlony w nowym oknie.

Kontrola aplikacji

Kontrola aplikacji zarządza uruchamianiem aplikacji na komputerach użytkowników. Pozwala to na wdrożenie polityki bezpieczeństwa firmy podczas korzystania z aplikacji. Kontrola aplikacji zmniejsza także ryzyko infekcji komputera poprzez ograniczenie dostępu do aplikacji.

Konfiguracja Kontroli aplikacji obejmuje następujące kroki:

1. [Tworzenia kategorii aplikacji.](#)

Administrator tworzy kategorie aplikacji, którymi chce zarządzać. Kategorie aplikacji są przeznaczone dla wszystkich komputerów w sieci firmowej, niezależnie od grup administracyjnych. Do utworzenia kategorii możesz użyć następujących kryteriów: kategoria KL (na przykład, *Przeglądarki*), suma kontrolna plików, producent aplikacji i inne kryteria.

2. [Tworzenie reguł Kontroli aplikacji.](#)

Administrator tworzy reguły Kontroli aplikacji w zasadzie dla grupy administracyjnej. Reguła obejmuje kategorie aplikacji i stan uruchamiania aplikacji z tych kategorii: zablokowane lub dozwolone.

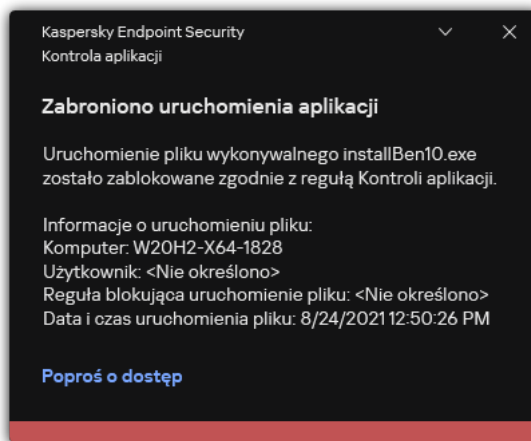
3. [Wybieranie trybu Kontroli aplikacji.](#)

Administrator wybiera tryb pracy z aplikacjami, które nie są uwzględnione w żadnej z reguł (lista zablokowanych i lista zezwolonych).

Jeśli użytkownik spróbuje uruchomić niedozwoloną aplikację, Kaspersky Endpoint Security zablokuje uruchomienie aplikacji i wyświetli powiadomienie (patrz rysunek poniżej).

Tryb testowy służy do sprawdzania konfiguracji Kontroli aplikacji. W tym trybie Kaspersky Endpoint Security wykonuje następujące czynności:

- Umożliwia uruchamianie aplikacji, w tym zabronionych.
- Wyświetla powiadomienie o uruchomieniu zabronionej aplikacji i dodaje informacje do raportu na komputerze użytkownika.
- Wysyła dane o uruchomieniu zabronionych aplikacji do Kaspersky Security Center.



Powiadomienie Kontroli aplikacji

Tryby działania Kontroli aplikacji

Komponent Kontrola aplikacji działa w dwóch trybach:

- **Lista zablokowanych.** W tym trybie Kontrola aplikacji umożliwia użytkownikom uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji zabronionych w regułach Kontroli aplikacji.

Ten tryb jest włączony domyślnie.

- **Lista zezwolonych.** W tym trybie Kontrola aplikacji blokuje użytkownikom możliwość uruchamiania dowolnych aplikacji, za wyjątkiem aplikacji, które są dozwolone i nie są zabronione w regułach Kontroli aplikacji.

Jeżeli reguły zezwalające Kontroli aplikacji zostaną w pełni skonfigurowane, moduł zablokuje uruchamianie wszystkich nowych aplikacji, które nie zostały zweryfikowane przez administratora sieci LAN, natomiast zezwoli na działanie systemu operacyjnego i zaufanych aplikacji potrzebnych użytkownikom w ich pracy.

Możesz przeczytać [zalecenia odnośnie konfiguracji reguł Kontroli aplikacji w trybie listy zezwolonych](#).

Moduł Kontrola aplikacji można skonfigurować do pracy w tych trybach, korzystając z lokalnego interfejsu Kaspersky Endpoint Security oraz programu Kaspersky Security Center.

Jednakże Kaspersky Security Center oferuje narzędzia, które nie są dostępne w lokalnym interfejsie Kaspersky Endpoint Security, a które są potrzebne do:

- [Tworzenia kategorii aplikacji](#).

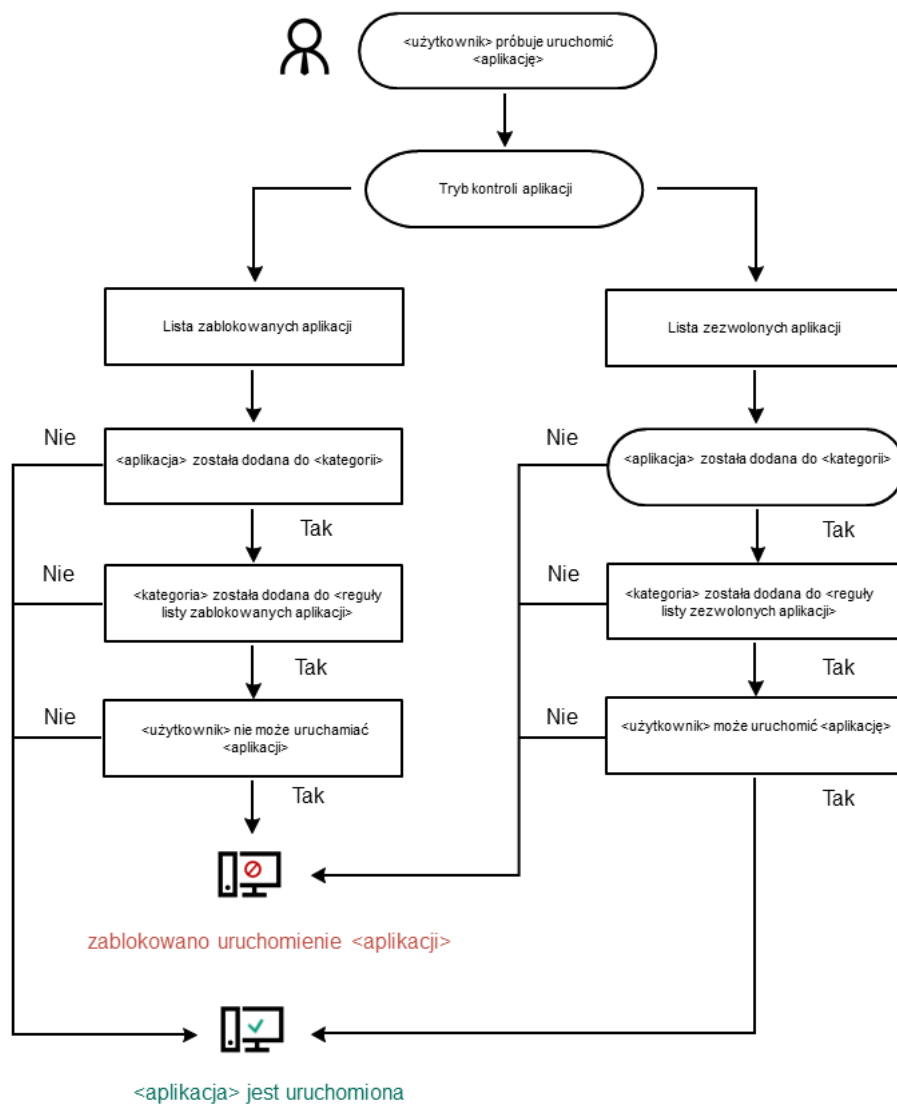
Reguły Kontroli aplikacji utworzone w Konsoli administracyjnej Kaspersky Security Center są oparte o niestandardowe kategorie aplikacji, a nie o warunki włączenia i wykluczenia, jak ma to miejsce w przypadku lokalnego interfejsu Kaspersky Endpoint Security.

- [Otrzymywania informacji o aplikacjach zainstalowanych na komputerach w korporacyjnej sieci LAN](#).

Dlatego zalecane jest korzystanie z Kaspersky Security Center podczas konfigurowania działania modułu Kontrola aplikacji.

Algorytm działania Kontroli aplikacji

Kaspersky Endpoint Security wykorzystuje algorytm do podjęcia decyzji o uruchomieniu aplikacji (patrz rysunek poniżej).



Algorytm działania Kontroli aplikacji

Ograniczenia funkcjonalności Kontroli aplikacji

Działanie komponentu Kontrola aplikacji jest ograniczone w następujących przypadkach:

- Jeśli wersja aplikacji zostanie zaktualizowana, importowanie ustawień komponentu Kontrola aplikacji nie będzie obsługiwane.
- Jeśli wersja aplikacji zostanie zaktualizowana, importowanie ustawień komponentu Kontrola aplikacji będzie obsługiwane tylko wtedy, gdy program Kaspersky Endpoint Security 10 Service Pack 2 for Windows lub w nowszych wersjach jest aktualizowany do Kaspersky Endpoint Security 11.7.0 for Windows.

Jeśli zostaną zaktualizowane wersje aplikacji inne niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows, ustawienia Kontroli aplikacji muszą zostać skonfigurowane na nowo w celu przywrócenia tego komponentu do stanu działania.

- Jeśli nie ma połączenia z serwerami KSN, Kaspersky Endpoint Security pobiera informacje o reputacji aplikacji i ich modułach z lokalnych baz danych.

Lista aplikacji, które Kaspersky Endpoint Security wskazuje jako kategorię **KL Inne aplikacje \ Aplikacje zaufane zgodnie z reputacją w KSN** może różnić się w zależności od tego, czy połączenie z serwerami KSN jest dostępne.

- Baza danych Kaspersky Security Center może przechowywać do 150 000 wpisów o przetworzonych plikach. Po osiągnięciu tej liczby wpisów, nowe pliki nie będą przetwarzane. Aby wznowić te działania, należy usunąć pliki, które były wcześniej przechowywane w bazie danych Kaspersky Security Center, z komputera, na którym jest zainstalowany program Kaspersky Endpoint Security.
- Komponent nie kontroluje uruchamiania skryptów, dopóki skrypt jest wysyłany do interpretera za pośrednictwem wiersza poleceń.

Jeśli uruchamianie interpretera jest dozwolone w regułach Kontroli aplikacji, komponent nie zablokuje uruchomienia skrypt z tego interpretera.

Jeśli uruchomienie przynajmniej jednego ze skryptów określonych w wierszu poleceń interpretera zostanie zablokowane przez reguły Kontroli aplikacji, komponent zablokuje wszystkie skrypty, określone w wierszu poleceń interpretera.

- Komponent nie kontroluje uruchamiania skryptów z interpreterów, które nie są obsługiwane przez Kaspersky Endpoint Security.

Kaspersky Endpoint Security obsługuje następujące interpretery:

- Java
- PowerShell

Obsługiwane są następujące typy interpreterów:


- %ComSpec%;
- %SystemRoot%\system32\regedit.exe;
- %SystemRoot%\regedit.exe;
- %SystemRoot%\system32\regedt32.exe;
- %SystemRoot%\system32\cscript.exe;
- %SystemRoot%\system32\wscript.exe;
- %SystemRoot%\system32\msiexec.exe;
- %SystemRoot%\system32\mshta.exe;
- %SystemRoot%\system32\rundll32.exe;
- %SystemRoot%\system32\wwahost.exe;

- %SystemRoot%\syswow64\cmd.exe;
- %SystemRoot%\syswow64\regedit.exe;
- %SystemRoot%\syswow64\regedt32.exe;
- %SystemRoot%\syswow64\cscript.exe;
- %SystemRoot%\syswow64\wscript.exe;
- %SystemRoot%\syswow64\msiexec.exe;
- %SystemRoot%\syswow64\mshta.exe;
- %SystemRoot%\syswow64\rundll32.exe;
- %SystemRoot%\syswow64\wwahost.exe.

Włączanie i wyłączanie modułu Kontrola aplikacji

Domyślnie Kontrola aplikacji jest wyłączona.


W celu włączenia lub wyłączenia modułu Kontrola aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
3. Użyj przełącznika **Kontrola aplikacji**, aby włączyć lub wyłączyć komponent.
4. Zapisz swoje zmiany.

W wyniku tego działania, jeśli moduł Kontrola aplikacji jest włączony, aplikacja przekazuje informacje o uruchomionych plikach wykonywalnych do Kaspersky Security Center. W folderze **Pliki wykonywalne** możesz przejrzeć listę uruchomionych plików wykonywalnych w Kaspersky Security Center. Aby otrzymywać informacje o wszystkich plikach wykonywalnych zamiast tylko o uruchomionych plikach wykonywalnych, uruchom [zadanie Inwentaryzacja](#).

Wybieranie trybu Kontroli aplikacji

W celu wybrania trybu Kontroli aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
3. W sekcji **Tryb Kontroli uruchamiania aplikacji** wybierz jedną z następujących opcji:
 - **Lista zablokowanych**. Jeśli ta opcja jest zaznaczona, Kontrola aplikacji zezwala wszystkim użytkownikom na uruchomienie dowolnej aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł blokowania Kontroli aplikacji.

- **Lista zezwolonych.** Jeśli ta opcja jest zaznaczona, Kontrola aplikacji blokuje wszystkim użytkownikom możliwość uruchomienia jakiejkolwiek aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł zezwalających Kontroli aplikacji.

Reguła **Obraz systemu** oraz reguła **Zaufane programy aktualizujące** jest wstępnie definiowana dla trybu Lista zezwolonych. Te reguły Kontroli aplikacji odpowiadają kategoriom KL. Kategoria KL „Obraz systemu” obejmuje programy, które zapewniają normalne działanie systemu operacyjnego. Kategoria KL „Zaufane programy aktualizujące” zawiera programy aktualizujące dla większości zaufanych producentów oprogramowania. Nie możesz usunąć tych reguł. Ustawienia dla tych reguł nie mogą być modyfikowane. Domyślnie, reguła **Obraz systemu** jest włączona, a reguła **Zaufane programy aktualizujące** jest wyłączona. Wszyscy użytkownicy mogą uruchamiać aplikacje odpowiadające warunkom wyzwalającym te reguły.

Wszystkie reguły utworzone przy włączonym tym trybie są zapisywane po zmianie trybu, dzięki czemu reguły będą mogły zostać ponownie użyte. Aby wrócić do korzystania z tych reguł, należy wybrać odpowiedni tryb.

4. Na liście rozwijanej **Akcja podczas uruchamiania zablokowanych aplikacji** wybierz akcję, jaka zostanie wykonana przez moduł, gdy użytkownik spróbuje uruchomić aplikację, która jest blokowana przez reguły Kontroli aplikacji.
5. Zaznacz pole **Kontroluj ładowanie modułów DLL (znacznie zwiększa obciążenie systemu)**, jeśli chcesz, aby Kaspersky Endpoint Security monitorował wczytywanie modułów DLL, gdy użytkownicy uruchamiają aplikacje.

Informacje o module i aplikacji, która wczytała moduł, będą zapisywane w raporcie.

Kaspersky Endpoint Security monitoruje tylko moduły DLL i sterowniki ładowane po zaznaczeniu pola. Po zaznaczeniu pola uruchom komputer ponownie, aby Kaspersky Endpoint Security monitorował wszystkie moduły DLL i sterowniki, w tym te załadowane przed uruchomieniem Kaspersky Endpoint Security.

Po włączeniu funkcji kontrolowania wczytywania modułów DLL i sterowników, upewnij się, że w ustawieniach Kontroli aplikacji włączona jest jedna z następujących reguł: domyślna reguła **Obraz systemu** lub inna reguła, która zawiera kategorię KL „Zaufane certyfikaty” i zapewnia, że moduły DLL i sterowniki są ładowane przed uruchomieniem Kaspersky Endpoint Security. Włączanie kontroli ładowania modułów DLL i sterowników, gdy reguła **Obraz systemu** jest wyłączona, może spowodować niestabilność systemu operacyjnego.

Zalecane jest włączenie [ochrony hasłem](#) dla konfigurowania ustawień aplikacji, tak, aby możliwe było wyłączenie reguł blokujących uruchomienie krytycznych modułów DLL i sterowników, bez modyfikowania ustawień profilu Kaspersky Security Center.

6. Zapisz swoje zmiany.

Praca z regułami Kontroli aplikacji w interfejsie aplikacji

Kaspersky Endpoint Security kontroluje uruchamianie aplikacji przez użytkownika przy użyciu reguł. Reguła Kontroli aplikacji określa warunki wyzwalania reguły oraz działania wykonywane przez Kontrolę aplikacji, gdy reguła zostaje wyzwolona (zezwalanie na lub blokowanie uruchamianie aplikacji przez użytkowników).

Warunki wyzwalające regułę

Warunek wyzwalający regułę ma następującą zależność: „typ warunku – kryterium warunku – wartość warunku”. W oparciu o warunki wyzwalające regułę, Kaspersky Endpoint Security stosuje (lub nie stosuje) regułę do aplikacji.

W regułach używane są następujące typy warunków:

- *Warunki włączenia.* Kaspersky Endpoint Security stosuje regułę do aplikacji, jeśli aplikacja odpowiada przynajmniej jednemu warunkowi włączenia.
- *Warunki wykluczenia.* Kaspersky Endpoint Security nie stosuje reguły do aplikacji, jeśli aplikacja odpowiada przynajmniej jednemu warunkowi wykluczenia i nie odpowiada żadnemu warunkowi włączenia.

Warunki wyzwalające regułę są tworzone przy użyciu kryteriów. Do tworzenia reguł w Kaspersky Endpoint Security używane są następujące kryteria:

- Ścieżka do folderu zawierającego plik wykonywalny aplikacji lub ścieżka dostępu do pliku wykonywalnego aplikacji.
- Metadane: nazwa pliku wykonywalnego aplikacji, wersja pliku wykonywalnego aplikacji, nazwa aplikacji, wersja aplikacji, producent aplikacji.
- Suma kontrolna pliku wykonywalnego aplikacji.
- Certyfikat: wydawca, podmiot, odcisk palca.
- Włączenie aplikacji do kategorii KL.
- Lokalizacja pliku wykonywalnego aplikacji na nośniku wymiennym.

Wartość kryterium musi być określona dla każdego kryterium używanego w warunku. Jeśli parametry uruchamianej aplikacji odpowiadają wartościom kryteriów określonym w warunkach włączenia, reguła zostanie wyzwolona. W tym przypadku Kontrola aplikacji wykona akcję określoną w regule. Jeśli parametry aplikacji odpowiadają wartościom kryteriów określonych w warunku wykluczenia, Kontrola aplikacji nie kontroluje uruchamiania aplikacji.

Jeśli jako warunek wyzwalający regułę wybrałeś certyfikat, musisz być pewny, że ten certyfikat jest dodawany do zaufanego magazynu systemu na komputerze oraz sprawdzić [ustawienia korzystania z zaufanego magazynu systemu w aplikacji](#).

Decyzja podjęta przez komponent Kontrola aplikacji w momencie wyzwolenia reguły

Jeśli reguła zostanie wyzwolona, Kontrola aplikacji zezwala użytkownikom (lub grupom użytkowników) na uruchamianie aplikacji lub blokuje uruchomienie zgodnie z regułą. Możesz wybrać pojedynczego użytkownika lub grupę użytkowników, którzy mogą (lub nie mogą) uruchamiać aplikacje wyzwalające regułę.

Jeśli reguła nie określa tych użytkowników mogących uruchamiać aplikacje odpowiadające regule, reguła ta jest zwana regułą *blokującą*.

Jeśli reguła, która nie określa żadnych użytkowników, którzy nie mogą uruchamiać aplikacji odpowiadających regule, reguła ta jest zwana regułą *zezwalającą*.

Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Na przykład, jeśli reguła zezwalająca kontroli aplikacji została określona dla grupy użytkowników, a dla użytkownika w tej grupie użytkowników określono regułę blokującą, nie będzie on mógł uruchamiać aplikacji.


Stan działania reguły

Reguły Kontroli aplikacji mogą posiadać jeden z następujących stanów działania:

- **Włączona.** Ten stan oznacza, że reguła jest używana, gdy działa Kontrola aplikacji.
- **Wyłączona.** Ten stan oznacza, że reguła jest ignorowana, gdy działa Kontrola aplikacji.
- **Sprawdź.** Ten stan oznacza, że Kaspersky Endpoint Security zezwala na uruchamianie aplikacji, do których reguły są stosowane, ale rejestrują informacje o uruchamianiu takich aplikacji w raporcie.

Dodawanie reguły Kontroli aplikacji

W celu dodania reguły Kontroli aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
3. Kliknij przycisk **Blokowane aplikacje** lub **Dozwolone aplikacje**.
Spowoduje to otwarcie listy reguł Kontroli aplikacji.
4. Kliknij przycisk **Dodaj**.
Zostanie otwarte okno **Reguła kontroli aplikacji**.
5. Na zakładce **Ustawienia główne** zdefiniuj główne ustawienia reguły:
 - a. W polu **Nazwa reguły** wprowadź nazwę reguły.
 - b. W polu **Opis** wprowadź opis reguły.
 - c. Utwórz lub zmodyfikuj listę użytkowników i/lub grup użytkowników, dla których będzie dozwolone lub zabronione uruchamianie aplikacji spełniających warunki wyzwalające regułę. Aby to zrobić, kliknij przycisk **Dodaj** w tabeli **Użytkownicy i ich uprawnienia**.
Domyślnie wartość **Wszyscy** jest dodana do listy użytkowników. Reguła jest stosowana do wszystkich użytkowników.

Jeśli w tabeli nie ma określonego użytkownika, reguła nie może zostać zapisana.

 - d. W tabeli **Użytkownicy i ich uprawnienia** użyj przełącznika do zdefiniowania uprawnienia użytkowników do uruchamiania aplikacji.
 - e. Wybierz pole **Zabroń innym użytkownikom**, jeśli chcesz, aby dla wszystkich użytkowników, którzy nie pojawiają się w kolumnie **Temat** i nie są częścią grupy użytkowników określonej w kolumnie **Temat**, została zablokowana możliwość uruchamiania aplikacji, które spełniają warunki wyzwalające regułę.

Jeśli pole **Zabroń innym użytkownikom** jest odznaczone, Kaspersky Endpoint Security nie kontroluje uruchamiania aplikacji przez użytkowników, którzy nie są określani w tabeli **Użytkownicy i ich uprawnienia** i nie należą do grup użytkowników określonych w tabeli **Użytkownicy i ich uprawnienia**.

f. Jeżeli chcesz, aby Kaspersky Endpoint Security uważał aplikacje spełniające warunki wyzwalające regułę za zaufane programy aktualizujące mogące tworzyć inne pliki wykonywalne, których uruchomienie będzie dozwolone, zaznacz pole **Zaufane programy aktualizujące**.

6. Na zakładce **Warunki** [utwórz](#) lub edytuj listę warunków włączenia wyzwalających regułę.


7. Na zakładce **Wykluczenia** utwórz lub edytuj listę warunków wykluczenia wyzwalających regułę.

Jeśli przenosisz ustawienia Kaspersky Endpoint Security, lista plików wykonywalnych utworzonych przez zaufane programy aktualizujące także zostanie przeniesiona.

8. Zapisz swoje zmiany.

Dodawanie warunku wyzwalającego dla reguły Kontroli aplikacji

W celu dodania nowego warunku wyzwalającego dla reguły Kontroli aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
3. Kliknij przycisk **Blokowane aplikacje** lub **Dozwolone aplikacje**.
Spowoduje to otwarcie listy reguł Kontroli aplikacji.
4. Wybierz regułę, dla której chcesz skonfigurować warunek wyzwalający.
Zostanie otwarte okno właściwości reguły Kontroli aplikacji.
5. Wybierz zakładkę **Warunki** lub zakładkę **Wykluczenia** i kliknij przycisk **Dodaj**.
6. Wybierz warunki wyzwalające dla reguły Kontroli aplikacji:
 - **Warunki z właściwości uruchomionych aplikacji**. Na liście uruchomionych aplikacji możesz wybrać aplikacje, do których zostanie zastosowana reguła Kontroli aplikacji. Kaspersky Endpoint Security wyświetla także aplikacje, które były wcześniej uruchomione na komputerze. Musisz wybrać kryterium, którego chcesz użyć do utworzenia jednego lub kilku warunków wyzwalających regułę: **Suma kontrolna pliku**, **Certyfikat**, **Kategoria KL**, **Metadane** lub **Ścieżka do folderu**.
 - **Warunki „Kategorii KL”**. *Kategoria KL* to lista aplikacji, które mają podobne atrybuty. Lista jest tworzona przez specjalistów z Kaspersky. Na przykład, kategoria KL „Aplikacje biurowe” zawiera aplikacje pakietu Microsoft Office, Adobe® Acrobat® i wiele innych.
 - **Warunek niestandardowy**. Możesz wybrać plik aplikacji oraz wybrać jeden z warunków wyzwalających regułę: **Suma kontrolna pliku**, **Certyfikat**, **Metadane** lub **Ścieżka do folderu**.
 - **Warunek według nośnika plików (dysk wymienny)**. Reguła Kontroli aplikacji jest stosowana tylko do plików, które są uruchamiane na nośniku wymiennym.
 - **Warunki z właściwości plików w określonym folderze**. Reguła Kontroli aplikacji jest stosowana tylko do plików w obrębie określonego folderu. Możesz także włączyć lub wykluczyć pliki z podfolderów. Musisz

wybrać kryterium, którego chcesz użyć do utworzenia jednego lub kilku warunków wyzwalających regułę: **Suma kontrolna pliku**, **Certyfikat**, **Kategoria KL**, **Metadane** lub **Ścieżka do folderu**.


7. Zapisz swoje zmiany.

Podczas dodawania warunków należy uwzględnić następujące specjalne właściwości Kontroli aplikacji:

- Kaspersky Endpoint Security nie obsługuje sumy kontrolnej pliku MD5 i nie kontroluje uruchamiania aplikacji w oparciu o sumę kontrolną MD5. Jako warunek wyzwalający regułę używana jest suma kontrolna SHA256.
- Nie jest zalecane używanie tylko elementów **Wydawca** i **Temat** jako warunków wyzwalających regułę. Użycie tych kryteriów jest niemiarodajne.
- Jeśli używasz dowiązania symbolicznego, w polu **Ścieżka do pliku lub folderu** zalecane jest rozwiązanie dowiązania symbolicznego w celu poprawnego działania reguły Kontroli aplikacji. W tym celu kliknij przycisk **Rozwiąż dowiązanie symboliczne**.

Zmianie stanu reguły Kontroli aplikacji

W celu zmiany stanu reguły Kontroli aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
3. Kliknij przycisk **Blokowane aplikacje** lub **Dozwolone aplikacje**.
Spowoduje to otwarcie listy reguł Kontroli aplikacji.
4. W kolumnie **Stan** otwórz menu kontekstowe i wybierz jeden z następujących elementów:
 - **Włączona**. Ten stan oznacza, że przy włączonym komponencie Kontrola aplikacji reguła ta jest wykorzystywana.
 - **Wyłączona**. Ten stan oznacza, że reguła jest ignorowana, gdy działa komponent Kontrola aplikacji.
 - **Testowanie**. Ten stan oznacza, że Kaspersky Endpoint Security zawsze zezwala na uruchamianie aplikacji, do których ta reguła jest stosowana, ale zapisuje informacje o uruchamianiu takich aplikacji w raporcie.
5. Zapisz swoje zmiany.

Zarządzanie regułami Kontroli aplikacji w Kaspersky Security Center

Kaspersky Endpoint Security kontroluje uruchamianie aplikacji przez użytkownika przy użyciu reguł. Reguła Kontroli aplikacji określa warunki wyzwalania reguły oraz działania wykonywane przez Kontrolę aplikacji, gdy reguła zostaje wyzwolona (zezwolenie na lub blokowanie uruchamianie aplikacji przez użytkowników).

Warunki wyzwalające regułę

Warunek wyzwalający regułę ma następującą zależność: „typ warunku - kryterium warunku - wartość warunku”. W oparciu o warunki wyzwalające regułę, Kaspersky Endpoint Security stosuje (lub nie stosuje) regułę do aplikacji.

W regułach używane są następujące typy warunków:

- *Warunki włączenia.* Kaspersky Endpoint Security stosuje regułę do aplikacji, jeśli aplikacja odpowiada przynajmniej jednemu warunkowi włączenia.
- *Warunki wykluczenia.* Kaspersky Endpoint Security nie stosuje reguły do aplikacji, jeśli aplikacja odpowiada przynajmniej jednemu warunkowi wykluczenia i nie odpowiada żadnemu warunkowi włączenia.

Warunki wyzwalające regułę są tworzone przy użyciu kryteriów. Do tworzenia reguł w Kaspersky Endpoint Security używane są następujące kryteria:

- Ścieżka do folderu zawierającego plik wykonywalny aplikacji lub ścieżka dostępu do pliku wykonywalnego aplikacji.
- Metadane: nazwa pliku wykonywalnego aplikacji, wersja pliku wykonywalnego aplikacji, nazwa aplikacji, wersja aplikacji, producent aplikacji.
- Suma kontrolna pliku wykonywalnego aplikacji.
- Certyfikat: wydawca, podmiot, odcisk palca.
- Włączenie aplikacji do kategorii KL.
- Lokalizacja pliku wykonywalnego aplikacji na nośniku wymiennym.

Wartość kryterium musi być określona dla każdego kryterium używanego w warunku. Jeśli parametry uruchamianej aplikacji odpowiadają wartościom kryteriów określonym w warunkach włączenia, reguła zostanie wyzwolona. W tym przypadku Kontrola aplikacji wykona akcję określoną w regule. Jeśli parametry aplikacji odpowiadają wartościom kryteriów określonych w warunku wykluczenia, Kontrola aplikacji nie kontroluje uruchamiania aplikacji.

Jeśli jako warunek wyzwalający regułę wybrałeś certyfikat, musisz być pewny, że ten certyfikat jest dodawany do zaufanego magazynu systemu na komputerze oraz sprawdzić [ustawienia korzystania z zaufanego magazynu systemu w aplikacji](#).

Decyzja podjęta przez komponent Kontrola aplikacji w momencie wyzwolenia reguły

Jeśli reguła zostanie wyzwolona, Kontrola aplikacji zezwala użytkownikom (lub grupom użytkowników) na uruchamianie aplikacji lub blokuje uruchomienie zgodnie z regułą. Możesz wybrać pojedynczego użytkownika lub grupę użytkowników, którzy mogą (lub nie mogą) uruchamiać aplikacje wyzwalające regułę.

Jeśli reguła nie określa tych użytkowników mogących uruchamiać aplikacje odpowiadające regule, reguła ta jest zwana regułą *blokującą*.

Jeśli reguła, która nie określa żadnych użytkowników, którzy nie mogą uruchamiać aplikacji odpowiadających regule, reguła ta jest zwana regułą *zezwalającą*.

Priorytet reguły blokującej jest wyższy niż priorytet reguły zezwalającej. Na przykład, jeśli reguła zezwalająca Kontroli aplikacji została określona dla grupy użytkowników, a dla użytkownika w tej grupie użytkowników określono regułę blokującą, nie będzie on mógł uruchamiać aplikacji.

Stan działania reguły

Reguły Kontroli aplikacji mogą posiadać jeden z następujących stanów działania:

- **Włączona.** Ten stan oznacza, że reguła jest używana, gdy działa Kontrola aplikacji.
- **Wyłączona.** Ten stan oznacza, że reguła jest ignorowana, gdy działa Kontrola aplikacji.

Sprawdź. Ten stan oznacza, że Kaspersky Endpoint Security zezwala na uruchamianie aplikacji, do których reguły są stosowane, ale rejestrują informacje o uruchamianiu takich aplikacji w raporcie.

Otrzymywanie informacji o aplikacjach zainstalowanych na komputerach użytkowników

Aby utworzyć optymalne reguły Kontroli aplikacji, najpierw należy zastanowić się, które aplikacje są używane na komputerach w korporacyjnej sieci LAN. W tym celu można wykorzystać następujące informacje o:

- Producentach, wersjach i lokalizacjach aplikacji używanych w firmowej sieci LAN.
- Częstotliwości aktualizacji aplikacji.
- Zasadach korzystania z aplikacji (mogą to być zasady zabezpieczeń lub zasady administracyjne).
- Lokalizacji magazynu pakietów dystrybucyjnych aplikacji.

Informacje o aplikacjach używanych na komputerach w firmowej sieci LAN są dostępne w folderze **Rejestr aplikacji** oraz w folderze **Pliki wykonywalne**. Folder **Rejestr aplikacji** i folder **Pliki wykonywalne** znajdują się w folderze **Zarządzanie aplikacjami**, dostępnym w drzewie Konsoli administracyjnej Kaspersky Security Center.

Folder **Rejestr aplikacji** zawiera listę aplikacji wykrytych przez [Agenta sieciowego](#), zainstalowanego na komputerze klienckim.

Folder **Pliki wykonywalne** zawiera listę wszystkich plików wykonywalnych, które kiedykolwiek były uruchomione na komputerach klienckich lub zostały wykryte podczas wykonywania zadania inwentaryzacji programu Kaspersky Endpoint Security.

Aby przejrzeć ogólne informacje o aplikacji i jej plikach wykonywalnych oraz listę komputerów, na których jest zainstalowana aplikacja, otwórz okno właściwości aplikacji wybranej w folderze **Rejestr aplikacji** lub **Pliki wykonywalne**.

*W celu otwarcia okna właściwości aplikacji w folderze **Rejestr aplikacji**:*

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz **Dodatkowe** → **Zarządzanie aplikacjami** → **Rejestr aplikacji**.
3. Wybierz aplikację.
4. Z menu kontekstowego aplikacji wybierz **Właściwości**.

*W celu otwarcia okna właściwości dla pliku wykonywalnego w folderze **Pliki wykonywalne**:*

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz folder **Dodatkowe** → **Zarządzanie aplikacjami** → **Pliki wykonywalne**.

3. Wybierz plik wykonywalny.

4. Z otwartego menu kontekstowego pliku wykonywalnego wybierz **Właściwości**.

Tworzenie kategorii aplikacji

Aby tworzenie reguł Kontroli aplikacji było wygodniejsze, możesz utworzyć kategorie aplikacji.

Zalecane jest utworzenie kategorii "Aplikacje do pracy", do której będzie należeć standardowy zestaw aplikacji używanych w firmie. Jeżeli różne grupy użytkowników używają w swojej pracy różnych zestawów aplikacji, dla każdej grupy użytkowników można utworzyć oddzielną kategorię aplikacji.

W celu utworzenia kategorii aplikacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz folder **Dodatkowe** → **Zarządzanie aplikacjami** → **Kategorie aplikacji**.
3. W obszarze roboczym kliknij **Nowa kategoria**.
Zostanie uruchomiony Kreator tworzenia kategorii użytkownika.
4. Postępuj zgodnie z instrukcjami Kreatora tworzenia kategorii użytkownika.

Krok 1. Wybieranie typu kategorii

W tym kroku wybierz jeden z następujących typów kategorii aplikacji:

- **Kategoria z zawartością dodaną ręcznie.** Jeśli wybrałeś ten typ kategorii, w kroku „Konfigurowanie warunków uwzględniania aplikacji w kategorii” oraz w kroku „Konfigurowanie warunków wykluczenia aplikacji z kategorii” będziesz mógł zdefiniować kryteria, za sprawą których pliki wykonywalne będą uwzględniane w kategorii.
- **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń.** Jeśli wybrałeś ten typ kategorii, w kroku „Ustawienia” będziesz mógł określić komputer, którego pliki wykonywalne zostaną automatycznie uwzględnione w kategorii.
- **Kategoria zawierająca pliki wykonywalne z określonego folderu.** Jeśli wybrałeś ten typ kategorii, w kroku „Folder Repozytorium” będziesz mógł określić folder, z którego pliki wykonywalne będą automatycznie uwzględniane w kategorii.

Podczas tworzenia kategorii z zawartością dodaną automatycznie Kaspersky Security Center przeprowadza inwentaryzację plików z następującymi formatami: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX i SCR.

Krok 2. Wprowadzanie nazwy kategorii użytkownika

W tym kroku określ nazwę kategorii aplikacji.

Krok 3. Konfigurowanie warunków uwzględniania aplikacji w kategorii

Ten krok jest dostępny, jeśli wybrałeś typ kategorii **Kategoria z zawartością dodaną ręcznie**.

W tym kroku, z listy rozwijalnej **Dodaj** wybierz warunki uwzględnienia aplikacji w kategorii:

- **Z listy plików wykonywalnych.** Dodaj aplikacje z listy plików wykonywalnych na urządzeniu klienckim do kategorii niestandardowej.
- **Z właściwości pliku.** Określ szczegółowe dane plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Metadane z plików w folderze.** Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne. Kaspersky Security Center wskaże metadane tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Sumy kontrolne plików znajdujących się w folderze.** Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne. Kaspersky Security Center wskaże sumy kontrolne tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Certyfikaty dla plików z folderu.** Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne podpisane certyfikatami. Kaspersky Security Center wskaże certyfikaty tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.

Nie jest zalecane używanie warunków, których właściwości nie posiadają określonego parametru **Odcisk palca certyfikatu**.

- **Metadane plików instalatora MSI.** Wybierz pakiet MSI. Kaspersky Security Center wskaże metadane plików wykonywalnych spakowanych w pakiecie MSI jako warunek dodania aplikacji do kategorii niestandardowej.
- **Sumy kontrolne plików z instalatora MSI aplikacji.** Wybierz pakiet MSI. Kaspersky Security Center wskaże sumy kontrolne plików wykonywalnych spakowanych w pakiecie MSI jako warunek dodania aplikacji do kategorii niestandardowej.
- **Z kategorii KL.** Określ kategorię KL jako warunek dodania aplikacji do kategorii niestandardowej. *Kategoria KL* to lista aplikacji, które mają podobne atrybuty. Lista jest tworzona przez specjalistów z Kaspersky. Na przykład, kategoria KL „Aplikacje biurowe” zawiera aplikacje pakietu Microsoft Office, Adobe Acrobat i wiele innych. Możesz wybrać wszystkie kategorie KL do wygenerowania rozszerzonej listy zaufanych aplikacji.
- **Określ ścieżkę do aplikacji.** Wybierz folder na urządzeniu klienckim. Kaspersky Security Center doda pliki wykonywalne z tego folderu do kategorii niestandardowej.
- **Wybierz certyfikat z repozytorium.** Wybierz certyfikaty, które zostały użyte do podpisania plików wykonywalnych, jako warunek dodania aplikacji do kategorii niestandardowej.

Nie jest zalecane używanie warunków, których właściwości nie posiadają określonego parametru **Odcisk palca certyfikatu**.

- **Typ dysku.** Określ typ urządzenia magazynującego (wszystkie dyski twarde i dyski wymienne lub tylko dyski wymienne) jako warunek dodania aplikacji do kategorii niestandardowej.

Krok 4. Konfigurowanie warunków wykluczenia aplikacji z kategorii

Ten krok jest dostępny, jeśli wybrałeś typ kategorii **Kategoria z zawartością dodaną ręcznie**.

Aplikacje określone w tym kroku zostaną wykluczone z kategorii nawet wtedy, gdy te aplikacje zostały określone w kroku „Konfigurowanie warunków uwzględniania aplikacji w kategorii”.

W tym kroku, z listy rozwijalnej **Dodaj** wybierz warunki wykluczania aplikacji z kategorii:

- **Z listy plików wykonywalnych.** Dodaj aplikacje z listy plików wykonywalnych na urządzeniu klienckim do kategorii niestandardowej.
- **Z właściwości pliku.** Określ szczegółowe dane plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Metadane z plików w folderze.** Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne. Kaspersky Security Center wskaże metadane tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Sumy kontrolne plików znajdujących się w folderze.** Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne. Kaspersky Security Center wskaże sumy kontrolne tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Certyfikaty dla plików z folderu.** Wybierz folder na urządzeniu klienckim, który zawiera pliki wykonywalne podpisane certyfikatami. Kaspersky Security Center wskaże certyfikaty tych plików wykonywalnych jako warunek dodania aplikacji do kategorii niestandardowej.
- **Metadane plików instalatora MSI.** Wybierz pakiet MSI. Kaspersky Security Center wskaże metadane plików wykonywalnych spakowanych w pakiecie MSI jako warunek dodania aplikacji do kategorii niestandardowej.
- **Sumy kontrolne plików z instalatora MSI aplikacji.** Wybierz pakiet MSI. Kaspersky Security Center wskaże sumy kontrolne plików wykonywalnych spakowanych w pakiecie MSI jako warunek dodania aplikacji do kategorii niestandardowej.
- **Z kategorii KL.** Określ kategorię KL jako warunek dodania aplikacji do kategorii niestandardowej. *Kategoria KL* to lista aplikacji, które mają podobne atrybuty. Lista jest tworzona przez specjalistów z Kaspersky. Na przykład, kategoria KL „Aplikacje biurowe” zawiera aplikacje pakietu Microsoft Office, Adobe Acrobat i wiele innych. Możesz wybrać wszystkie kategorie KL do wygenerowania rozszerzonej listy zaufanych aplikacji.
- **Określ ścieżkę do aplikacji.** Wybierz folder na urządzeniu klienckim. Kaspersky Security Center doda pliki wykonywalne z tego folderu do kategorii niestandardowej.
- **Wybierz certyfikat z repozytorium.** Wybierz certyfikaty, które zostały użyte do podpisania plików wykonywalnych, jako warunek dodania aplikacji do kategorii niestandardowej.
- **Typ dysku.** Określ typ urządzenia magazynującego (wszystkie dyski twarde i dyski wymienne lub tylko dyski wymienne) jako warunek dodania aplikacji do kategorii niestandardowej.

Krok 5. Ustawienia

Ten krok jest dostępny, jeśli wybrałeś typ kategorii **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń**.

W tym kroku kliknij przycisk **Dodaj** i określ komputery, których pliki wykonywalne zostaną dodane do kategorii aplikacji przez Kaspersky Security Center. Wszystkie pliki wykonywalne z określonych komputerów, znajdujące się w folderze [Pliki wykonywalne](#), zostaną dodane do kategorii aplikacji przez Kaspersky Security Center.

W tym kroku możesz skonfigurować następujące ustawienia:

- Algorytm obliczania funkcji skrótu przez Kaspersky Security Center. W celu wybrania algorytmu musisz zaznaczyć przynajmniej jedną z następujących opcji:
 - **Oblicz sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze).**
 - **Oblicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane przez starsze wersje niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows).**
- **Synchronizuj dane z repozytorium Serwera administracyjnego.** Zaznacz to pole, jeśli chcesz, żeby Kaspersky Security Center okresowo czyścił kategorię aplikacji i dodawał do niej wszystkie pliki wykonywalne z określonych komputerów, znajdujących się w folderze **Pliki wykonywalne**.

Jeśli pole **Synchronizuj dane z repozytorium Serwera administracyjnego** jest odznaczone, Kaspersky Security Center nie wprowadzi żadnych modyfikacji do kategorii aplikacji po jej utworzeniu.

- Pole **Okres skanowania (godz.)**. W tym polu możesz określić czas (w godzinach), po jakim Kaspersky Security Center wyczyści kategorię aplikacji i doda do niej wszystkie pliki wykonywalne z określonych komputerów, znajdujących się w folderze **Pliki wykonywalne**.

Pole jest dostępne, jeśli zaznaczona jest opcja **Synchronizuj dane z repozytorium Serwera administracyjnego**.

Krok 6. Folder Repozytorium

Ten krok jest dostępny, jeśli wybrałeś typ kategorii **Kategoria zawierająca pliki wykonywalne z określonego folderu**.

W tym kroku kliknij przycisk **Przełączaj** i określ folder, w którym Kaspersky Security Center wyszuka pliki wykonywalne do automatycznego dodania aplikacji do kategorii aplikacji.

W tym kroku możesz skonfigurować następujące ustawienia:

- **Uwzględnij w tej kategorii biblioteki dołączane dynamicznie (DLL).** Zaznacz to pole, jeśli chcesz, aby biblioteki dołączane dynamicznie (pliki DLL) były uwzględnione w kategorii aplikacji.

Uwzględnienie plików DLL w kategorii aplikacji może zmniejszyć wydajność Kaspersky Security Center.

- **Uwzględnij w tej kategorii dane skryptów.** Zaznacz to pole, jeśli chcesz, aby skrypty były uwzględniane w kategorii aplikacji.

Uwzględnienie skryptów w kategorii aplikacji może zmniejszyć wydajność Kaspersky Security Center.

- Algorytm obliczania funkcji skrótu przez Kaspersky Security Center. W celu wybrania algorytmu musisz zaznaczyć przynajmniej jedną z następujących opcji:
 - **Oblicz sumy SHA-256 plików należących do tej kategorii (obsługiwane przez Kaspersky Endpoint Security 10 Service Pack 2 for Windows i nowsze).**

- Oblicz sumę kontrolną MD5 dla plików z tej kategorii (obsługiwane przez starsze wersje niż Kaspersky Endpoint Security 10 Service Pack 2 for Windows).
- **Wymuś skanowanie folderu pod kątem zmian.** Zaznacz to pole, jeśli chcesz, żeby Kaspersky Security Center okresowo wyszukiwał pliki wykonywalne w folderze używanym do automatycznego dodawania do kategorii aplikacji.
Jeśli pole **Wymuś skanowanie folderu pod kątem zmian** jest odznaczone, Kaspersky Security Center wyszukuje pliki wykonywalne w folderze używanym do automatycznego dodawania do kategorii aplikacji tylko wtedy, gdy w folderze zostały wprowadzone zmiany, pliki zostały dodane do niego lub zostały usunięte z niego.
- Pole **Okres skanowania (godz.)**. W tym polu możesz określić przedział czasu (w godzinach), po jakim Kaspersky Security Center rozpocznie wyszukiwanie plików wykonywalnych w folderze używanym do automatycznego dodawania do kategorii aplikacji.
To pole jest dostępne, jeśli opcja **Wymuś skanowanie folderu pod kątem zmian** jest zaznaczona.

Krok 7. Tworzenie kategorii niestandardowej

W celu zakończenia pracy z Kreatorem instalacji aplikacji kliknij przycisk **Zakończ**.

Dodawanie plików wykonywalnych z folderu Pliki wykonywalne do kategorii aplikacji

W folderze **Pliki wykonywalne** zostanie wyświetlona lista plików wykonywalnych wykrytych na komputerach. Kaspersky Endpoint Security wygeneruje listę plików wykonywalnych po wykonaniu zadania inwentaryzacji.

*W celu dodania plików wykonywalnych z folderu **Pliki wykonywalne** do kategorii aplikacji:*

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz folder **Dodatkowe** → **Zarządzanie aplikacjami** → **Pliki wykonywalne**.
3. W obszarze roboczym wybierz pliki wykonywalne, które chcesz dodać do kategorii aplikacji.
4. Kliknij wybrany plik wykonywalny prawym klawiszem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Dodaj do kategorii**.
5. W otwartym oknie wykonaj jedną z następujących czynności:
 - W górnej części okna wybierz jedną z poniższych opcji:
 - **Dodaj do nowej kategorii aplikacji.** Wybierz tę opcję, jeśli chcesz utworzyć nową kategorię aplikacji i dodać do niej pliki wykonywalne.
 - **Dodaj do istniejącej kategorii aplikacji.** Wybierz tę opcję, jeśli chcesz wybrać istniejącą kategorię aplikacji i dodać do niej pliki wykonywalne.
 - W sekcji **Typ reguły** wybierz jedną z następujących opcji:
 - **Reguły dodawania do włączeń.** Wybierz tę opcję, jeśli chcesz utworzyć warunek, który dodaje pliki wykonywalne do kategorii aplikacji.

- **Reguły dodawania do wykluczeń.** Wybierz tę opcję, jeśli chcesz utworzyć warunek, który wyklucza pliki wykonywalne z kategorii aplikacji.
- W sekcji **Parametr użyty jako warunek** wybierz jedną z następujących opcji:
 - **Szczegóły certyfikatu (lub sumy kontrolne SHA-256 dla plików bez certyfikatu).**
 - **Szczegóły certyfikatu (pliki bez certyfikatu zostaną pominięte).**
 - **Tylko SHA-256 (pliki bez sumy kontrolnej zostaną pominięte).**
 - **Tylko MD5 (tryb wycofany, wyłącznie dla Kaspersky Endpoint Security 10 Service Pack 1).**

6. Kliknij **OK**.

Dodawanie plików wykonywalnych związanych ze zdarzeniami do kategorii aplikacji

W celu dodania plików wykonywalnych związanych ze zdarzeniami Kontroli aplikacji do kategorii aplikacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Zdarzenia**.
3. Wybierz wybór zdarzeń związanych z działaniem komponentu Kontrola aplikacji ([Przeglądanie zdarzeń z działania modułu Kontrola aplikacji](#), [Przeglądanie zdarzeń z działania testowego komponentu Kontrola aplikacji](#)) z listy rozwijalnej **Wybory zdarzeń**.
4. Kliknij przycisk **Uruchom wybrane**.
5. Wybierz zdarzenia, których skojarzone pliki wykonywalne chcesz dodać do kategorii aplikacji.
6. Kliknij wybrane zdarzenia prawym klawiszem myszy, aby otworzyć menu kontekstowe, z którego wybierz **Dodaj do kategorii**.
7. W otwartym oknie skonfiguruj ustawienia kategorii aplikacji:
 - W górnej części okna wybierz jedną z poniższych opcji:
 - **Dodaj do nowej kategorii aplikacji.** Wybierz tę opcję, jeśli chcesz utworzyć nową kategorię aplikacji i dodać do niej pliki wykonywalne.
 - **Dodaj do istniejącej kategorii aplikacji.** Wybierz tę opcję, jeśli chcesz wybrać istniejącą kategorię aplikacji i dodać do niej pliki wykonywalne.
 - W sekcji **Typ reguły** wybierz jedną z następujących opcji:
 - **Reguły dodawania do włączeń.** Wybierz tę opcję, jeśli chcesz utworzyć warunek, który dodaje pliki wykonywalne do kategorii aplikacji.
 - **Reguły dodawania do wykluczeń.** Wybierz tę opcję, jeśli chcesz utworzyć warunek, który wyklucza pliki wykonywalne z kategorii aplikacji.

- W sekcji **Parametr użyty jako warunek** wybierz jedną z następujących opcji:
 - **Szczegóły certyfikatu (lub sumy kontrolne SHA-256 dla plików bez certyfikatu).**
 - **Szczegóły certyfikatu (pliki bez certyfikatu zostaną pominięte).**
 - **Tylko SHA-256 (pliki bez sumy kontrolnej zostaną pominięte).**
 - **Tylko MD5 (tryb wycofany, wyłącznie dla Kaspersky Endpoint Security 10 Service Pack 1).**

8. Kliknij **OK**.

Dodawanie i modyfikowanie reguły Kontroli aplikacji przy użyciu Kaspersky Security Center

W celu dodania lub zmodyfikowania reguły Kontroli aplikacji przy użyciu Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
W prawej części okna wyświetlone są ustawienia modułu Kontrola aplikacji.
6. Wykonaj jedną z poniższych czynności:
 - W celu dodania reguły kliknij przycisk **Dodaj**.
 - Jeśli chcesz zmodyfikować istniejącą regułę, wybierz ją na liście reguł i kliknij przycisk **Edytuj**.

To spowoduje otwarcie okna **Reguły Kontroli aplikacji**.

7. Wykonaj jedną z poniższych czynności:
 - Jeśli chcesz utworzyć nową kategorię:
 - a. Kliknij przycisk **Utwórz kategorię**.
Zostanie uruchomiony Kreator tworzenia kategorii użytkownika.
 - b. Postępuj zgodnie z instrukcjami Kreatora tworzenia kategorii użytkownika.
 - c. Z listy rozwijalnej **Kategoria** wybierz utworzoną kategorię aplikacji.
 - Jeśli chcesz edytować istniejącą kategorię:
 - a. Z listy rozwijalnej **Kategoria** wybierz utworzoną kategorię aplikacji, którą chcesz edytować.

b. Kliknij przycisk **Właściwości**.

c. Zmodyfikuj ustawienia wybranej kategorii aplikacji.

d. Kliknij **OK**.

e. Z listy rozwijalnej **Kategoria** wybierz utworzoną kategorię aplikacji, w oparciu o którą chcesz utworzyć regułę.

8. W tabeli **Użytkownicy i ich uprawnienia** kliknij przycisk **Dodaj**.

9. W oknie **Wybierz Użytkowników lub Grupy** określ listę użytkowników i/lub grup użytkowników, dla których chcesz skonfigurować uprawnienia uruchamiania aplikacji z wybranej kategorii.

10. W tabeli **Użytkownicy i ich uprawnienia**:

- Jeśli chcesz zezwolić użytkownikom i/lub grupom użytkowników na uruchamianie aplikacji, które należą do wybranej kategorii, zaznacz pola **Zezwól** obok odpowiednich wierszy.
- Jeśli chcesz zablokować użytkownikom i/lub grupom użytkowników możliwość uruchamiania aplikacji, które należą do wybranej kategorii, zaznacz pola **Odmów** obok odpowiednich wierszy.

11. Wybierz pole **Zabroń innym użytkownikom**, jeśli chcesz, aby dla wszystkich użytkowników, którzy nie pojawiają się w kolumnie **Użytkownik** i nie są częścią grupy użytkowników określonej w kolumnie **Użytkownik**, została zablokowana możliwość uruchamiania aplikacji, które należą do wybranej kategorii.

12. Jeżeli chcesz, aby Kaspersky Endpoint Security uważał aplikacje znajdujące się w wybranej kategorii aplikacji za zaufane programy aktualizujące mogące tworzyć inne pliki wykonywalne, których uruchomienie będzie dozwolone, zaznacz pole **Zaufane programy aktualizujące**.

Jeśli przenosisz ustawienia Kaspersky Endpoint Security, lista plików wykonywalnych utworzonych przez zaufane programy aktualizujące także zostanie przeniesiona.

13. Zapisz swoje zmiany.

Zmianie stanu reguły Kontroli aplikacji przy użyciu Kaspersky Security Center

W celu zmiany stanu reguły Kontroli aplikacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
W prawej części okna wyświetlone są ustawienia modułu Kontrola aplikacji.

6. W kolumnie **Stan** kliknij lewym klawiszem myszy, aby wyświetlić menu kontekstowe, z którego wybierz jeden z następujących elementów:

- **Włączona**. Ten stan oznacza, że reguła jest używana, gdy działa Kontrola aplikacji.
- **Wyłączona**. Ten stan oznacza, że reguła jest ignorowana, gdy działa Kontrola aplikacji.
- **Testowa**. Ten stan oznacza, że Kaspersky Endpoint Security zawsze zezwala na uruchamianie aplikacji, do których reguła jest stosowana, ale zapisuje informacje o uruchamianiu takich aplikacji w raporcie.

Możesz użyć stanu **Testowa** do przypisania [akcji Przetestuj reguły](#) dla niektórych reguł, jeśli z listy rozwijalnej **Akcja** wybrano opcję **Zastosuj reguły**.

7. Zapisz swoje zmiany.

Eksportowanie i importowanie reguł Kontroli aplikacji

Możesz wyeksportować listę reguł Kontroli aplikacji do pliku XML. Możesz użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy reguł Kontroli aplikacji lub przeniesienia listy na inny serwer.

Podczas eksportowania i importowania reguł Kontroli aplikacji należy mieć na uwadze następujące kwestie specjalne:

- Kaspersky Endpoint Security eksportuje listę reguł tylko dla aktywnego trybu Kontroli aplikacji. Innymi słowy, jeśli Kontrola aplikacji działa w trybie listy zabronionych, Kaspersky Endpoint Security eksportuje reguły tylko dla tego trybu. Aby wyeksportować listę reguł dla trybu listy zezwolonych, należy przełączyć tryb i uruchomić eksportowanie ponownie.
- Kaspersky Endpoint Security używa kategorii aplikacji dla działania reguł Kontroli aplikacji. Podczas przenoszenia listy reguł Kontroli aplikacji na inny serwer, musisz także przenieść listę kategorii aplikacji. Więcej informacji dotyczących eksportowania lub importowania kategorii aplikacji można znaleźć w [pomocy do Kaspersky Security Center](#).

[Eksportowanie i importowanie listy reguł Kontroli aplikacji w Konsoli administracyjnej \(MMC\)](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
6. W celu wyeksportowania listy reguł Kontroli aplikacji:
 - a. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.
7. W celu wyeksportowania reguł Kontroli aplikacji:
 - a. Kliknij odnośnik **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
 - b. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.

[Eksportowanie i importowanie listy reguł Kontroli aplikacji w Web Console i Cloud Console](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listę reguł.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
5. Kliknij odnośnik **Ustawienia list reguł**.
6. Wybierz listę reguł: lista zablokowanych i lista zezwolonych aplikacji.
7. W celu wyeksportowania listy reguł Kontroli aplikacji:
 - a. Wybierz reguły, które chcesz zmienić.
 - b. Kliknij przycisk **Eksportuj**.
 - c. Potwierdź chęć wyeksportowania tylko wybranych reguł lub wyeksportuj całą listę.
 - d. Kliknij przycisk **Eksportuj**.
Kaspersky Endpoint Security eksportuje listę reguł do pliku XML w domyślnym folderze do pobrania.
8. W celu wyeksportowania reguł Kontroli aplikacji:
 - a. Kliknij odnośnik **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
 - b. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
9. Zapisz swoje zmiany.

Testowanie reguł Kontroli aplikacji przy użyciu Kaspersky Security Center

Aby upewnić się, że reguły Kontroli aplikacji nie będą blokowały aplikacji niezbędnych do pracy, po utworzeniu nowych reguł zalecane jest włączenie testowania reguł Kontroli aplikacji i sprawdzenie ich działania. Jeśli testowanie reguł Kontroli aplikacji jest włączone, Kaspersky Endpoint Security nie zablokuje aplikacji, których uruchamianie jest zabronione przez Kontrolę aplikacji, ale zamiast tego wyśle informacje o ich uruchomieniu do Serwera administracyjnego.

Analiza działania reguł Kontroli aplikacji obejmuje przejrzanie zdarzeń Kontroli aplikacji zgłoszonych do Kaspersky Security Center. Jeśli wyniki trybu testowego wykazały zdarzenia, w których nie zostały zablokowane uruchomienia wszystkich aplikacji wymaganych do pracy użytkownika komputera, oznacza to, że zostały utworzone poprawne reguły. W innej sytuacji zalecane jest zaktualizowanie ustawień utworzonych reguł, utworzenie dodatkowych reguł oraz usunięcie istniejących reguł.

Domyślnie Kaspersky Endpoint Security pozwala na uruchomienie wszystkich aplikacji, za wyjątkiem aplikacji zabronionych przez reguły.

W celu włączenia lub wyłączenia testowania reguł Kontroli aplikacji w Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
W prawej części okna wyświetlone są ustawienia modułu Kontrola aplikacji.
6. Z listy rozwijalnej **Tryb kontroli** wybierz jeden z następujących elementów:
 - **Lista zablokowanych.** Jeśli ta opcja jest zaznaczona, Kontrola aplikacji zezwala wszystkim użytkownikom na uruchomienie dowolnej aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł blokowania Kontroli aplikacji.
 - **Lista zezwolonych.** Jeśli ta opcja jest zaznaczona, Kontrola aplikacji blokuje wszystkim użytkownikom możliwość uruchomienia jakiejkolwiek aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł zezwalających Kontroli aplikacji.
7. Wykonaj jedną z poniższych czynności:
 - Jeśli chcesz włączyć testowanie reguł Kontroli aplikacji, z listy rozwijalnej **Akcja** wybierz opcję **Zastosuj reguły**.
 - Jeśli chcesz włączyć Kontrolę aplikacji do zarządzania uruchamianiem aplikacji na komputerach użytkowników, z listy rozwijalnej wybierz **Zastosuj reguły**.
8. Zapisz swoje zmiany.

Przeglądanie zdarzeń z działania testowego komponentu Kontrola aplikacji

W celu przejrzania zdarzeń testowych Kontroli aplikacji otrzymanych przez Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Zdarzenia**.
3. Kliknij przycisk **Utwórz wybór**.
Zostanie otwarte okno **Właściwości: <nazwa wyboru>**.
4. Otwórz sekcję **Zdarzenia**.
5. Kliknij przycisk **Wyczyść wszystko**.

6. W tabeli **Zdarzenia** zaznacz pola **Zabroniono uruchomienia aplikacji w trybie testowym** i **Zezwolono na uruchomienie aplikacji w trybie testowym**.
7. Kliknij **OK**.
8. Z listy rozwijalnej **Wybory zdarzeń** wybierz utworzony wybór.
9. Kliknij przycisk **Uruchom wybrane**.

Przeglądanie raportu dotyczącego zablokowanych aplikacji w trybie testowym

W celu wyświetlenia raportu dotyczącego zablokowanych aplikacji w trybie testowym:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Raporty**.
3. Kliknij przycisk **Nowy szablon raportu**.
Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu.
4. Postępuj zgodnie z instrukcjami Kreatora szablonu raportu. W kroku **Wybieranie typu szablonu raportu** wybierz **Inne** → **Raport o zabronionych aplikacjach w trybie testowym**.
Po zakończeniu pracy Kreatora nowego szablonu raportu, nowy szablon raportu pojawi się w tabeli, na zakładce **Raporty**.
5. Otwórz raport, klikając go dwukrotnie.

Zostanie rozpoczęty proces tworzenia raportu. Raport zostanie wyświetlony w nowym oknie.

Przeglądanie zdarzeń z działania modułu Kontrola aplikacji

W celu przejrzania zdarzeń wynikających z działania komponentu Kontrola aplikacji, otrzymanych przez Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Zdarzenia**.
3. Kliknij przycisk **Utwórz wybór**.
Zostanie otwarte okno **Właściwości: <nazwa wyboru>**.
4. Otwórz sekcję **Zdarzenia**.
5. Kliknij przycisk **Wyczyść wszystko**.
6. W tabeli **Zdarzenia** zaznacz pole **Zabroniono uruchomienia aplikacji**.
7. Kliknij **OK**.

8. Z listy rozwijalnej **Wybory zdarzeń** wybierz utworzony wybór.

9. Kliknij przycisk **Uruchom wybrane**.

Przeglądanie raportu dotyczącego zablokowanych aplikacji

W celu wyświetlenia raportu dotyczącego zablokowanych aplikacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Raporty**.

3. Kliknij przycisk **Nowy szablon raportu**.

Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu.

4. Postępuj zgodnie z instrukcjami Kreatora szablonu raportu. W kroku **Wybieranie typu szablonu raportu** wybierz **Inne** → **Raport o zabronionych aplikacjach**.

Po zakończeniu pracy Kreatora nowego szablonu raportu, nowy szablon raportu pojawi się w tabeli, na zakładce **Raporty**.

5. Otwórz raport, klikając go dwukrotnie.

Zostanie rozpoczęty proces tworzenia raportu. Raport zostanie wyświetlony w nowym oknie.

Testowanie działania reguł Kontroli aplikacji

Aby upewnić się, że reguły Kontroli aplikacji nie będą blokowały aplikacji niezbędnych do pracy, po utworzeniu nowych reguł zalecane jest włączenie testowania reguł Kontroli aplikacji i sprawdzenie ich działania.

Analiza działania reguł Kontroli aplikacji obejmuje przejrzanie zdarzeń Kontroli aplikacji zgłoszonych do Kaspersky Security Center. Jeśli wyniki trybu testowego wykazały zdarzenia, w których nie zostały zablokowane uruchomienia wszystkich aplikacji wymaganych do pracy użytkownika komputera, oznacza to, że zostały utworzone poprawne reguły. W innej sytuacji zalecane jest zaktualizowanie ustawień utworzonych reguł, utworzenie dodatkowych reguł oraz usunięcie istniejących reguł.

W celu włączenia testowania reguł Kontroli aplikacji lub wybrania akcji blokowania dla Kontroli aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.

Spowoduje to otwarcie listy reguł Kontroli aplikacji.

3. W kolumnie **Stan** wybierz **Testowanie**.

Ten stan oznacza, że Kaspersky Endpoint Security zawsze zezwala na uruchamianie aplikacji, do których ta reguła jest stosowana, ale zapisuje informacje o uruchamianiu takich aplikacji w raporcie.

4. Zapisz swoje zmiany.

Kaspersky Endpoint Security nie zablokuje aplikacji, których uruchamianie jest zabronione przez komponent Kontroli aplikacji, ale wyśle informacje o ich uruchomieniu do Serwera administracyjnego.

Monitor aktywności aplikacji

Monitor aktywności aplikacji to narzędzie służące do wyświetlania informacji o aktywności aplikacji na komputerze użytkownika w czasie rzeczywistym.

Używanie Monitora aktywności aplikacji wymaga zainstalowania komponentów Kontrola aplikacji i Ochrona przed włamaniami. Jeśli te komponenty nie są zainstalowane, sekcja Monitor aktywności aplikacji w [oknie głównym aplikacji](#) jest ukryta.

W celu Monitor aktywności aplikacji:

W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Monitor aktywności aplikacji**.

Zostanie otwarte okno **Aktywność aplikacji**. W tym oknie informacje o aktywności aplikacji na komputerze użytkownika są przedstawione na trzech zakładkach:

- Zakładka **Wszystkie aplikacje** wyświetla informacje o wszystkich aplikacjach zainstalowanych na komputerze.
- Zakładka **Uruchomione** wyświetla informacje o zużyciu zasobów komputera według każdej aplikacji w czasie rzeczywistym. Z poziomu tej zakładki może także przejść do konfigurowania uprawnień dla pojedynczej aplikacji.
- Zakładka **Uruchomione przy starcie** wyświetla listę aplikacji, które są uruchamiane podczas uruchamiania systemu operacyjnego.

Jeśli chcesz ukryć informacje o aktywności aplikacji na komputerze użytkownika, możesz ograniczyć dostęp użytkownika do narzędzia Monitor aktywności aplikacji.

[Jak w interfejsie aplikacji ukryć Monitor aktywności aplikacji, korzystając z Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Ustawienia główne** → **Interfejs**.
6. Użyj pola **Ukryj sekcję Monitor aktywności aplikacji**, aby nadać lub wycofać dostęp do narzędzia.
7. Zapisz swoje zmiany.

[Jak w interfejsie aplikacji ukryć Monitor aktywności aplikacji, korzystając z Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia główne** → **Interfejs**.
5. Użyj pola **Ukryj sekcję Monitor aktywności aplikacji**, aby nadać lub wycofać dostęp do narzędzia.
6. Zapisz swoje zmiany.

Reguły tworzenia masek nazw dla plików i folderów

Maska nazwy pliku lub folderu to reprezentacja nazwy folderu lub nazwy i rozszerzenia pliku przy użyciu ogólnych znaków.

Do utworzenia maski nazwy pliku lub folderu można użyć następujących popularnych znaków:


- Znak ***** (gwiazdka), który zastępuje dowolny zestaw znaków (w tym pusty zestaw). Na przykład, maska `C:*.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem `txt`, znajdujących się w folderach i podfolderach na dysku (C:).
- Znak **?** (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie `TXT` i nazwę składającą się z trzech znaków.

Modyfikowanie szablonów wiadomości Kontroli aplikacji

Podczas próby uruchomienia aplikacji, zablokowanej przez regułę Kontroli aplikacji, program Kaspersky Endpoint Security wyświetli wiadomość informująca o zablokowaniu uruchomienia aplikacji. Jeżeli użytkownik ma pewność, że uruchomienie aplikacji zostało zablokowane przez pomyłkę, powinien użyć odnośnika dostępnego w wiadomości w celu przesłania zgłoszenia do administratora lokalnej sieci firmowej.

Dostępne są specjalne szablony dla wiadomości wyświetlanej, gdy zostaje zablokowane uruchomienie aplikacji, oraz dla wiadomości wysyłanej do administratora. Możesz zmodyfikować szablony wiadomości.

W celu zmodyfikowania szablonu wiadomości:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Kontrola zabezpieczeń** → **Kontrola aplikacji**.
3. W sekcji **Szablony** skonfiguruj szablony dla wiadomości Kontroli aplikacji:

- **Wiadomość dotycząca blokowania.** Szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła Kontroli aplikacji, która blokuje uruchamianie aplikacji.
- **Wiadomość do administratora.** Szablon wiadomości, którą użytkownik może wysłać do administratora korporacyjnej sieci LAN, jeśli uważa, że aplikacja została przypadkowo zablokowana. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania uruchomienia aplikacji** Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkowników**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

4. Zapisz swoje zmiany.

Praktyczne zastosowanie aplikacji w celu zaimplementowania listy dozwolonych aplikacji

Podczas planowania implementacji listy zezwolonych aplikacji zalecane jest wykonanie następujących działań:

1. Utwórz następujące typy grup:

- Grupy użytkowników. Grupy użytkowników, dla których musisz zezwolić na korzystanie z różnych zestawów aplikacji.
- Grupy administracyjne. Jeden lub kilka grup komputerów, do których Kaspersky Security Center zastosuje listę zezwolonych aplikacji. Konieczne jest utworzenie kilku grup komputerów, jeśli dla tych grup zostały użyte różne ustawienia listy zezwolonych.

2. Utworzenie listy aplikacji, których uruchamianie musi być dozwolone.

Przed utworzeniem listy, zalecane jest wykonanie następujących czynności:

a. Uruchom zadanie inwentaryzacji.

Informacje o utworzeniu, ponownej konfiguracji i uruchomieniu zadania inwentaryzacji są dostępne w sekcji Zarządzanie zadaniami.

b. Przejrzyj [listę plików wykonywalnych](#).

Konfigurowanie trybu listy zezwolonych aplikacji

Podczas konfigurowania trybu listy zezwolonych zalecane jest wykonanie następujących działań:

1. Utworzenie [kategorii aplikacji](#) zawierających aplikacje, których uruchamianie ma być dozwolone.

Możesz wybrać jedną z następujących metod tworzenia kategorii aplikacji:

- **Kategoria z zawartością dodaną ręcznie.** Możesz ręcznie dodać tę kategorię, korzystając z następujących warunków:
 - Metadane plików. Kaspersky Security Center doda wszystkie pliki wykonywalne z określonymi metadanymi do kategorii aplikacji.

- Suma kontrolna pliku. Kaspersky Security Center doda wszystkie pliki wykonywalne z określoną sumą kontrolną do kategorii aplikacji.

Użycie tego warunku wykluczy możliwość automatycznego zainstalowania uaktualnień, ponieważ różne wersje plików będą posiadać różne sumy kontrolne.

- Certyfikat pliku. Kaspersky Security Center doda wszystkie pliki wykonywalne podpisane określonym certyfikatem do kategorii aplikacji.
- Kategoria KL. Kaspersky Security Center doda wszystkie aplikacje, które znajdują się w określonej kategorii KL, do kategorii aplikacji.
- Folder aplikacji. Kaspersky Security Center doda wszystkie pliki wykonywalne z tego folderu do kategorii aplikacji.

Użycie warunku Folder aplikacji może nie być bezpieczne, ponieważ każda aplikacja z określonego folderu będzie mogła być uruchamiana. Zalecane jest zastosowanie reguł, które używają kategorii aplikacji z warunkiem Folder aplikacji, tylko do tych użytkowników, dla których musi być dozwolona automatyczna instalacja uaktualnień.

- **Kategoria zawierająca pliki wykonywalne z określonego folderu.** Możesz określić folder, z którego pliki wykonywalne będą automatycznie przydzielane do utworzonej kategorii aplikacji.
- **Kategoria zawierająca pliki wykonywalne z wybranych urządzeń.** Możesz określić komputer, z którego wszystkie pliki wykonywalne będą automatycznie przydzielane do utworzonej kategorii aplikacji.

Jeśli użyjesz tej metody do utworzenia kategorii aplikacji, Kaspersky Security Center będzie otrzymywał informacje o aplikacjach na komputerze z [folderu Pliki wykonywalne](#).

2. [Wybierz tryb listy zezwolonych](#) dla komponentu Kontrola aplikacji.

3. [Utwórz reguły Kontroli aplikacji](#), korzystając z utworzonych kategorii aplikacji.

Reguła **Obraz systemu** oraz reguła **Zaufane programy aktualizujące** jest wstępnie definiowana dla trybu Lista zezwolonych. Te reguły Kontroli aplikacji odpowiadają kategoriom KL. Kategoria KL „Obraz systemu” obejmuje programy, które zapewniają normalne działanie systemu operacyjnego. Kategoria KL „Zaufane programy aktualizujące” zawiera programy aktualizujące dla większości zaufanych producentów oprogramowania. Nie możesz usunąć tych reguł. Ustawienia dla tych reguł nie mogą być modyfikowane. Domyślnie, reguła **Obraz systemu** jest włączona, a reguła **Zaufane programy aktualizujące** jest wyłączona. Wszyscy użytkownicy mogą uruchamiać aplikacje odpowiadające warunkom wyzwającym te reguły.

4. Określ aplikacje, dla których dozwolona musi być automatyczna instalacja uaktualnień.

Możesz zezwolić na automatyczną instalację uaktualnień w jeden z następujących sposobów:

- Określ rozszerzoną listę dozwolonych aplikacji, zezwalając na uruchamianie wszystkich aplikacji, które należą do dowolnej kategorii KL.
- Określ rozszerzoną listę dozwolonych aplikacji, zezwalając na uruchamianie wszystkich aplikacji, które są podpisane certyfikatami.

Aby zezwolić na uruchomienie wszystkich aplikacji podpisanych certyfikatami, możesz utworzyć kategorię z warunkiem opartym o certyfikat, który używa tylko parametru **Podmiot** z wartością *.

- Dla reguł Kontroli aplikacji wybierz parametr **Zaufane programy aktualizujące**. Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security traktuje aplikacje, uwzględnione w regule, jako Zaufane programy aktualizujące. Kaspersky Endpoint Security zezwala na uruchamianie aplikacji, które zostały zainstalowane lub zaktualizowane przez aplikacje uwzględnione w regule, jeśli nie są do nich stosowane żadne reguły blokujące.

Jeśli przenosisz ustawienia Kaspersky Endpoint Security, lista plików wykonywalnych utworzonych przez zaufane programy aktualizujące także zostanie przeniesiona.

- Utwórz folder i umieść w nim pliki wykonywalne aplikacji, dla których chcesz zezwolić na automatyczną instalację aktualizacji. Następnie utwórz kategorię aplikacji z warunkiem „Folder aplikacji” i określ ścieżkę do tego folderu. Kolejnym krokiem jest utworzenie reguły zezwalającej i wybranie tej kategorii.

Użycie warunku Folder aplikacji może nie być bezpieczne, ponieważ każda aplikacja z określonego folderu będzie mogła być uruchamiana. Zalecane jest zastosowanie reguł, które używają kategorii aplikacji z warunkiem Folder aplikacji, tylko do tych użytkowników, dla których musi być dozwolona automatyczna instalacja uaktualnień.

Testowanie trybu listy zezwolonych

Aby upewnić się, że reguły Kontroli aplikacji nie będą blokowały aplikacji niezbędnych do pracy, po utworzeniu nowych reguł zalecane jest włączenie testowania reguł Kontroli aplikacji i sprawdzenie ich działania. Jeśli testowanie jest włączone, Kaspersky Endpoint Security nie zablokuje aplikacji, których uruchamianie jest zabronione przez reguły Kontroli aplikacji, ale zamiast tego wyśle informacje o ich uruchomieniu do Serwera administracyjnego.

Podczas testowania listy zezwolonych zalecane jest wykonanie następujących działań:

1. Określenie okresu testowego (liczącego od kilku dni do dwóch miesięcy).
2. Włącz [testowanie reguł Kontroli aplikacji](#).
3. Sprawdź [zdarzenia będące wynikiem testowania działania Kontroli aplikacji](#) i [raporty dotyczące zablokowanych aplikacji w trybie testowym](#) w celu przeanalizowania wyników testu.
4. W oparciu o wyniki analizy, wprowadź zmiany w ustawieniach trybu listy zezwolonych.

W szczególności na podstawie wyników testu można dodać [pliki wykonywalne związane ze zdarzeniami do kategorii aplikacji](#).

Obsługa listy zezwolonych aplikacji

Po [wybraniu akcji blokowania dla Kontroli aplikacji](#), zalecane jest kontynuowanie wsparcia trybu listy zezwolonych poprzez wykonanie następujących czynności:

- [Sprawdź zdarzenia będące wynikiem działania Kontroli aplikacji](#) i [raporty dotyczące zablokowanych uruchomień](#) w celu przeanalizowania efektywności działania Kontroli aplikacji.
- Przeanalizuj prośby użytkowników o dostęp do aplikacji.
- Analizuj nieznanne pliki wykonywalne, sprawdzając ich reputację w [Kaspersky Security Network](#).

- Przed zainstalowaniem uaktualnień dla systemu operacyjnego lub dla oprogramowania, zainstaluj te uaktualnienia na testowej grupie komputerów, aby sprawdzić sposób ich przetwarzania przez reguły Kontroli aplikacji.
- Dodaj odpowiednie aplikacje do kategorii użytych w regułach Kontroli aplikacji.


Monitorowanie portów sieciowych

Podczas działania Kaspersky Endpoint Security komponenty [Kontrola sieci](#), [Ochrona poczty](#) i [Ochrona WWW](#) monitorują strumienie danych, które są przesyłane za pośrednictwem określonych protokołów i które przechodzą przez określone otwarte porty TCP i UDP na komputerze użytkownika. Na przykład, komponent Ochrona poczty analizuje informacje przesyłane poprzez protokół SMTP, a komponent Ochrona WWW analizuje informacje przesyłane poprzez protokół HTTP i FTP.

Kaspersky Endpoint Security dzieli porty TCP i UDP komputera użytkownika na kilka grup, w zależności od prawdopodobieństwa ich zagrożenia. Niektóre porty sieciowe są zarezerwowane dla usług podatnych na ataki. Zalecane jest monitorowanie tych portów z większą dokładnością, ponieważ istnieje większe prawdopodobieństwo, że staną się one celem ataku sieciowego. Jeśli korzystasz z niestandardowych usług polegających na niestandardowych portach, te porty sieciowe również mogą stać się celem atakującego komputera. Możesz określić listę portów sieciowych i listę aplikacji, które żądają dostępu do sieci. Te porty i aplikacje będą pod specjalnym nadzorem modułów Ochrona poczty i Ochrona WWW podczas monitorowania ruchu sieciowego.


Włączanie monitorowania wszystkich portów sieciowych

W celu włączenia monitorowania wszystkich portów sieciowych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.
3. W sekcji **Monitorowane porty** zaznacz opcję **Monitoruj wszystkie porty sieciowe**.
4. Zapisz swoje zmiany.

Tworzenie listy monitorowanych portów sieciowych

W celu utworzenia listy monitorowanych portów sieciowych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.
3. W sekcji **Monitorowane porty** zaznacz **Monitoruj tylko wybrane porty sieciowe**.
4. Kliknij przycisk **Wybierz**.

Spowoduje to otwarcie listy portów sieciowych, które są zazwyczaj używane do przesyłania ruchu sieciowego i pocztowego. Lista portów sieciowych jest zawarta w pakiecie Kaspersky Endpoint Security.

5. Użyj przełącznika w kolumnie **Stan**, aby włączyć lub wyłączyć monitorowanie portu sieciowego.
6. Jeśli port sieciowy nie jest wyświetlany na liście portów sieciowych, dodaj go w następujący sposób:
 - a. Kliknij przycisk **Dodaj**.
 - b. W otwartym oknie wprowadź numer portu sieciowego oraz krótki opis.
 - c. Ustaw stan **Aktywny** lub **Nieaktywny** dla monitorowania portu sieciowego.
7. Zapisz swoje zmiany.


Jeśli protokół FTP działa w trybie pasywnym, połączenie będzie można nawiązać poprzez losowy port sieciowy, który nie został dodany do listy monitorowanych portów sieciowych. Aby chronić takie połączenia, [włącz monitorowanie wszystkich portów sieciowych](#) lub [skonfiguruj kontrolę portów sieciowych dla aplikacji, które nawiązują połączenia z FTP](#).

Tworzenie listy aplikacji, dla których monitorowane są wszystkie porty sieciowe

Możesz utworzyć listę aplikacji, dla których Kaspersky Endpoint Security monitoruje wszystkie porty sieciowe.

Zalecamy uwzględnić aplikacje odbierające lub przesyłające dane przez protokół FTP na liście aplikacji, dla których Kaspersky Endpoint Security monitoruje wszystkie porty sieciowe.

W celu utworzenia listy aplikacji, dla których monitorowane są wszystkie porty sieciowe:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ustawienia sieciowe**.
3. W sekcji **Monitorowane porty** zaznacz **Monitoruj tylko wybrane porty sieciowe**.
4. Zaznacz pole **Monitoruj wszystkie porty dla aplikacji z listy zalecanej przez Kaspersky**.

Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security monitoruje wszystkie porty dla następujących aplikacji:

 - Adobe Reader.
 - Apple Application Support.
 - Google Chrome.
 - Microsoft Edge.
 - Mozilla Firefox.
 - Internet Explorer.
 - Java.

- mIRC.
- Opera.
- Pidgin.
- Safari.
- Mail.ru Agent.
- Yandex Browser.

5. Zaznacz pole **Monitoruj wszystkie porty dla określonych aplikacji**.

6. Kliknij przycisk **Wybierz**.

Spowoduje to otwarcie listy aplikacji, dla których Kaspersky Endpoint Security monitoruje porty sieciowe.

7. Użyj przełącznika w kolumnie **Stan**, aby włączyć lub wyłączyć monitorowanie portu sieciowego.

8. Jeśli aplikacja nie znajduje się na liście aplikacji, dodaj ją w następujący sposób:

- a. Kliknij przycisk **Dodaj**.
- b. W otwartym oknie wprowadź ścieżkę do pliku wykonywalnego aplikacji oraz krótki opis.
- c. Ustaw stan **Aktywny** lub **Nieaktywny** dla monitorowania portów sieciowych.

9. Zapisz swoje zmiany.

Eksportowanie i importowanie list monitorowanych portów

Kaspersky Endpoint Security używa następujących list monitorowania portów sieciowych: listy portów sieciowych i listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security. Możesz wyeksportować listy monitorowanych portów do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę portów z tym samym opisem. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej list monitorowanych portów lub przeniesienia list na inny serwer.

[Eksportowanie i importowanie list monitorowanych portów w Konsoli administracyjnej \(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Ustawienia główne** → **Ustawienia sieci**.
6. W sekcji **Monitorowane porty** zaznacz **Monitoruj tylko wybrane porty sieciowe**.
7. Kliknij przycisk **Ustawienia**.

Zostanie otwarte okno **Porty sieciowe**. W oknie **Porty sieciowe** wyświetlana jest lista portów sieciowych, które są zazwyczaj używane do przesyłania ruchu sieciowego i pocztowego. Lista portów sieciowych jest zawarta w pakiecie Kaspersky Endpoint Security.
8. W celu wyeksportowania listy portów sieciowych:
 - a. Z listy portów sieciowych wybierz porty, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

Jeśli nie wybrałeś żadnego portu, Kaspersky Endpoint Security wyeksportuje wszystkie porty.
 - b. Kliknij przycisk **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę portów sieciowych i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.

Kaspersky Endpoint Security eksportuje całą listę portów sieciowych do pliku XML.
9. W celu wyeksportowania listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security:
 - a. Zaznacz pole **Monitoruj wszystkie porty dla określonych aplikacji**.
 - b. Z listy aplikacji wybierz aplikacje, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.

Jeśli nie wybrałeś żadnej aplikacji, Kaspersky Endpoint Security wyeksportuje wszystkie aplikacje.
 - c. Kliknij przycisk **Eksportuj**.
 - d. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę aplikacji, i wybierz folder, w którym chcesz zapisać ten plik.
 - e. Kliknij przycisk **Zapisz**.

Kaspersky Endpoint Security wyeksportuje całą listę aplikacji do pliku XML.
10. W celu zaimportowania listy portów sieciowych:
 - a. Na liście portów sieciowych kliknij przycisk **Importuj**.

W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę portów sieciowych.

b. Kliknij przycisk **Otwórz**.

Jeśli komputer ma już listę portów sieciowych, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

11. W celu zaimportowania listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security:

a. Na liście aplikacji kliknij przycisk **Importuj**.

W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę aplikacji.

b. Kliknij przycisk **Otwórz**.

Jeśli komputer ma już listę aplikacji, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

12. Zapisz swoje zmiany.

[Eksportowanie / importowanie list monitorowanych portów w Web Console i Cloud Console](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listy monitorowanych portów.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do sekcji **Ustawienia główne** → **Ustawienia sieciowe**.
5. W celu wyeksportowania listy portów sieciowych:
 - a. W sekcji **Monitorowane porty** zaznacz **Monitoruj tylko wybrane porty sieciowe**.
 - b. Kliknij odnośnik **Wybrano N portów**.
Zostanie otwarte okno **Porty sieciowe**. W oknie **Porty sieciowe** wyświetlana jest lista portów sieciowych, które są zazwyczaj używane do przesyłania ruchu sieciowego i pocztowego. Lista portów sieciowych jest zawarta w pakiecie Kaspersky Endpoint Security.
 - c. Z listy portów sieciowych wybierz porty, które chcesz wyeksportować.
 - d. Kliknij przycisk **Eksportuj**.
 - e. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę portów sieciowych i wybierz folder, w którym chcesz zapisać ten plik.
 - f. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje całą listę portów sieciowych do pliku XML.
6. W celu wyeksportowania listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security:
 - a. W sekcji **Monitorowane porty** zaznacz pole **Monitoruj wszystkie porty dla określonych aplikacji**.
 - b. Kliknij odnośnik **Wybrano N aplikacji**.
 - c. Z listy aplikacji wybierz aplikacje, które chcesz wyeksportować.
 - d. Kliknij przycisk **Eksportuj**.
 - e. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę aplikacji, i wybierz folder, w którym chcesz zapisać ten plik.
 - f. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security wyeksportuje całą listę aplikacji do pliku XML.
7. W celu zaimportowania listy portów sieciowych:
 - a. Na liście portów sieciowych kliknij przycisk **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę portów sieciowych.
 - b. Kliknij przycisk **Otwórz**.

Jeśli komputer ma już listę portów sieciowych, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

8. W celu zaimportowania listy aplikacji, których porty są monitorowane przez Kaspersky Endpoint Security:

a. Na liście aplikacji kliknij przycisk **Importuj**.

W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę aplikacji.

b. Kliknij przycisk **Otwórz**.

Jeśli komputer ma już listę aplikacji, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.

9. Zapisz swoje zmiany.

Wyczyść dane

Kaspersky Endpoint Security umożliwia korzystanie z zadania do zdalnego usuwania danych z komputerów użytkowników.

Kaspersky Endpoint Security usuwa dane w następujący sposób:

- W trybie cichym;
- Na dyskach twardych i nośnikach wymiennych;
- Dla wszystkich kont użytkownika na komputerze.

Kaspersky Endpoint Security wykonuje zadanie *Wyczyść dane* niezależnie od tego, który typ licencjonowania jest używany, nawet po wygaśnięciu licencji.

Tryby czyszczenia danych

To zadanie umożliwia usuwanie danych w następujących trybach:

- Natychmiastowe usuwanie danych.
W tym trybie możliwe jest, na przykład, usunięcie przestarzałych danych w celu zwolnienia miejsca na dysku.
- Odroczone usuwanie danych.
Ten tryb jest przeznaczony, na przykład, do ochrony danych na laptopie w przypadku jego zgubienia lub kradzieży. Możesz skonfigurować automatyczne usuwanie danych, jeśli laptop znajdzie się poza granicami sieci firmowej i nie był zsynchronizowany z Kaspersky Security Center od dłuższego czasu.

Nie można ustawić terminarza usuwania danych we właściwościach zadania. Możesz usunąć dane natychmiast po ręcznym uruchomieniu zadania lub skonfigurować opóźnione usuwanie danych, jeśli nie ma połączenia z Kaspersky Security Center.

Ograniczenia

Czyszczenie danych posiada następujące ograniczenia:

- Tylko administrator Kaspersky Security Center może zarządzać zadaniem *Wyczyść dane*. Nie możesz skonfigurować ani uruchomić zadania w lokalnym interfejsie Kaspersky Endpoint Security.
- W systemie plików NTFS Kaspersky Endpoint Security usuwa tylko nazwy głównych strumieni danych. Alternatywnych nazw strumieni danych nie można usunąć.
- Po usunięciu pliku dowiązania symbolicznego, Kaspersky Endpoint Security usuwa również pliki, których ścieżki są określone w dowiązaniu symbolicznym.

Tworzenie zadania Wyczyść dane

W celu usunięcia danych na komputerach użytkowników:

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

b. Na liście rozwijalnej **Typ zadania** wybierz **Wyczyść dane**.

c. W polu **Nazwa zadania** wpisz krótki opis, na przykład, **Usuń dane (Anti-Theft)**.

d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.

Jeśli nowe komputery są dodawane do grupy administracyjnej w obrębie obszaru zadania, natychmiast zostaje uruchomione zadanie usuwania danych na nowych komputerach tylko wtedy, gdy zadanie zostaje zakończone w ciągu 5 minut od dodania nowych komputerów.

5. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

Nowe zadanie zostanie wyświetlone na liście zadań.

6. Wybierz zadanie **Wyczyść dane** programu Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości zadania.

7. Wybierz zakładkę **Ustawienia aplikacji**.

8. Wybierz metodę usuwania danych:

- **Usuń za pomocą systemu operacyjnego.** Kaspersky Endpoint Security używa zasobów systemu operacyjnego do usuwania plików bez wysyłania ich do kosza.
- **Usuń całkowicie, bez możliwości przywrócenia.** Kaspersky Endpoint Security nadpisuje pliki losowymi danymi. Przywrócenie danych po ich usunięciu jest praktycznie niemożliwe.

9. Jeśli chcesz odroczyć usunięcie danych, zaznacz pole **Automatycznie usuwaj dane w przypadku braku połączenia z Kaspersky Security Center dłuższego niż N dni**. Określ liczbę dni.

Odroczone zadanie usuwania danych zostanie wykonane za każdym razem, gdy nie ma połączenia z Kaspersky Security Center przez określony czas.

Podczas konfigurowania odroczonego usuwania danych należy pamiętać, że pracownicy mogą wyłączyć komputery przed wyjazdem na wakacje. W tym przypadku okres braku połączenia może zostać wydłużony, a dane zostaną usunięte. Należy także uwzględnić terminarz pracy użytkowników offline. Szczegółowe informacje na temat pracy z komputerami offline i użytkownikami mobilnymi *można znaleźć w [pomocy do Kaspersky Security Center](#)*.

Jeśli pole jest odznaczone, zadanie zostanie wykonane natychmiast po synchronizacji z Kaspersky Security Center.

10. Utwórz listę usuwanych obiektów:

- **Foldery.** Kaspersky Endpoint Security usunie wszystkie pliki w folderze i jego podfolderach. Kaspersky Endpoint Security nie obsługuje masek i zmiennych środowiskowych dla wprowadzania ścieżki dostępu do folderu.
- **Pliki według rozszerzenia.** Kaspersky Endpoint Security wyszukuje pliki z określonymi rozszerzeniami na wszystkich dyskach komputera, w tym dyskach wymiennych. Użyj znaku „;” lub „,”, aby określić kilka rozszerzeń.
- **Wstępnie określone foldery.** Kaspersky Endpoint Security usunie pliki z następujących obszarów:
 - **Dokumenty.** Pliki w standardowym folderze *Dokumenty* systemu operacyjnego i jego podfolderach.
 - **Ciasteczka.** Pliki, w których przeglądarka zapisuje dane ze stron internetowych odwiedzonych przez użytkownika (takie jak dane autoryzacyjne użytkownika).
 - **Pulpit.** Pliki w standardowym folderze *Pulpit* systemu operacyjnego i jego podfolderach.
 - **Pliki tymczasowe Internet Explorer.** Pliki tymczasowe związane z działaniem przeglądarki Internet Explorer, takie jak kopie stron internetowych, obrazów i plików multimedialnych.
 - **Pliki tymczasowe.** Pliki tymczasowe związane z działaniem aplikacji zainstalowanych na komputerze. Na przykład, aplikacje Microsoft Office tworzą pliki tymczasowe zawierające kopie zapasowe dokumentów.
 - **Pliki programu Outlook.** Pliki dotyczące działania klienta poczty Outlook: pliki danych (PST), pliki danych offline (OST), pliki książki adresowej offline (OAB) oraz pliki osobistej książki adresowej (PAB).
 - **Profil użytkownika.** Zestaw plików i folderów, które przechowują ustawienia systemu operacyjnego dla lokalnego konta użytkownika.

Możesz utworzyć listę obiektów do usunięcia na każdej zakładce. Kaspersky Endpoint Security utworzy skonsolidowaną listę i usunie pliki z tej listy po zakończeniu zadania.

Nie możesz usuwać plików wymaganych do działania Kaspersky Endpoint Security.

11. Kliknij przycisk **Zapisz**.

12. Zaznacz pole obok zadania.

13. Kliknij przycisk **Uruchom**.

W wyniku tego działania dane na komputerach użytkowników zostaną usunięte zgodnie z wybranym trybem: natychmiast lub gdy nie ma połączenia. Jeśli program Kaspersky Endpoint Security nie może usunąć pliku, gdy, na przykład, użytkownik aktualnie używa pliku, aplikacja nie podejmie kolejnej próby jego usunięcia. Aby zakończyć usuwanie danych, uruchom zadanie ponownie.

Ochrona hasłem

Zdarza się, że z jednego komputera korzysta wielu użytkowników o różnej umiejętności jego obsługi. Jeżeli użytkownicy nie mają ograniczonego dostępu do Kaspersky Endpoint Security i jego ustawień, może to zmniejszyć ogólny poziom ochrony komputera. Ochrona hasłem umożliwia ograniczenie dostępu użytkowników do Kaspersky Endpoint Security zgodnie z uprawnieniami im nadanymi (na przykład, uprawnienie do zakończenia działania aplikacji).

Jeśli użytkownik, który rozpoczął sesję Windows (*użytkownik sesji*) ma uprawnienia do wykonania tej akcji, Kaspersky Endpoint Security nie prosi o nazwę użytkownika i hasło ani o hasło tymczasowe. Użytkownik uzyskuje dostęp do Kaspersky Endpoint Security zgodnie z udzielonymi uprawnieniami.

Jeśli użytkownik sesji nie ma uprawnień do wykonania akcji, może uzyskać dostęp do aplikacji w następujące sposoby:

- Wprowadź nazwę użytkownika i hasło.

Ta metoda jest odpowiednia dla codziennych działań. Aby wykonać działanie chronione hasłem, musisz wprowadzić poświadczenia konta domeny użytkownika z wymaganym uprawnieniem. W takim przypadku komputer musi należeć do tej domeny. Jeśli komputer nie znajduje się w domenie, możesz użyć konta KLAdmin.

- Wprowadź hasło tymczasowe.

Ta metoda jest odpowiednia do nadania uprawnień tymczasowych do wykonywania zablokowanych działań (na przykład, kończenia działania aplikacji) użytkownikom poza siecią firmową. Jeśli hasło tymczasowe wygaśnie lub sesja zakończy się, Kaspersky Endpoint Security przywróci ustawienia do poprzedniego stanu.

Jeśli użytkownik spróbuje wykonać działanie ochrony hasłem, Kaspersky Endpoint Security wyświetli prośbę o podanie nazwy użytkownika i hasła lub hasła tymczasowego (patrz rysunek poniżej).

W oknie do wprowadzenia hasła możesz zmienić język tylko poprzez wciśnięcie klawiszy **ALT+SHIFT**. Korzystając z innych skrótów, nawet wtedy, gdy są skonfigurowane w systemie operacyjnym, nie działają do zmiany języków.

Kaspersky X

Jesteś pewien, że chcesz zmienić ustawienia?

Nazwa użytkownika:

Domyślna nazwa użytkownika: KLAdmin.

Wprowadź hasło:

Nie pytaj o potwierdzenie podczas kolejnych:
Pytaj za każdym razem

Aby przełączać się między językami, użyj ALT+SHIFT. **ENU**

Potwierdź Anuluj

Monit o podanie hasła dostępu do Kaspersky Endpoint Security

Nazwa użytkownika i hasło

Aby uzyskać dostęp do Kaspersky Endpoint Security, należy wprowadzić dane uwierzytelniające konta domeny. Ochrona hasłem obsługuje następujące konta:

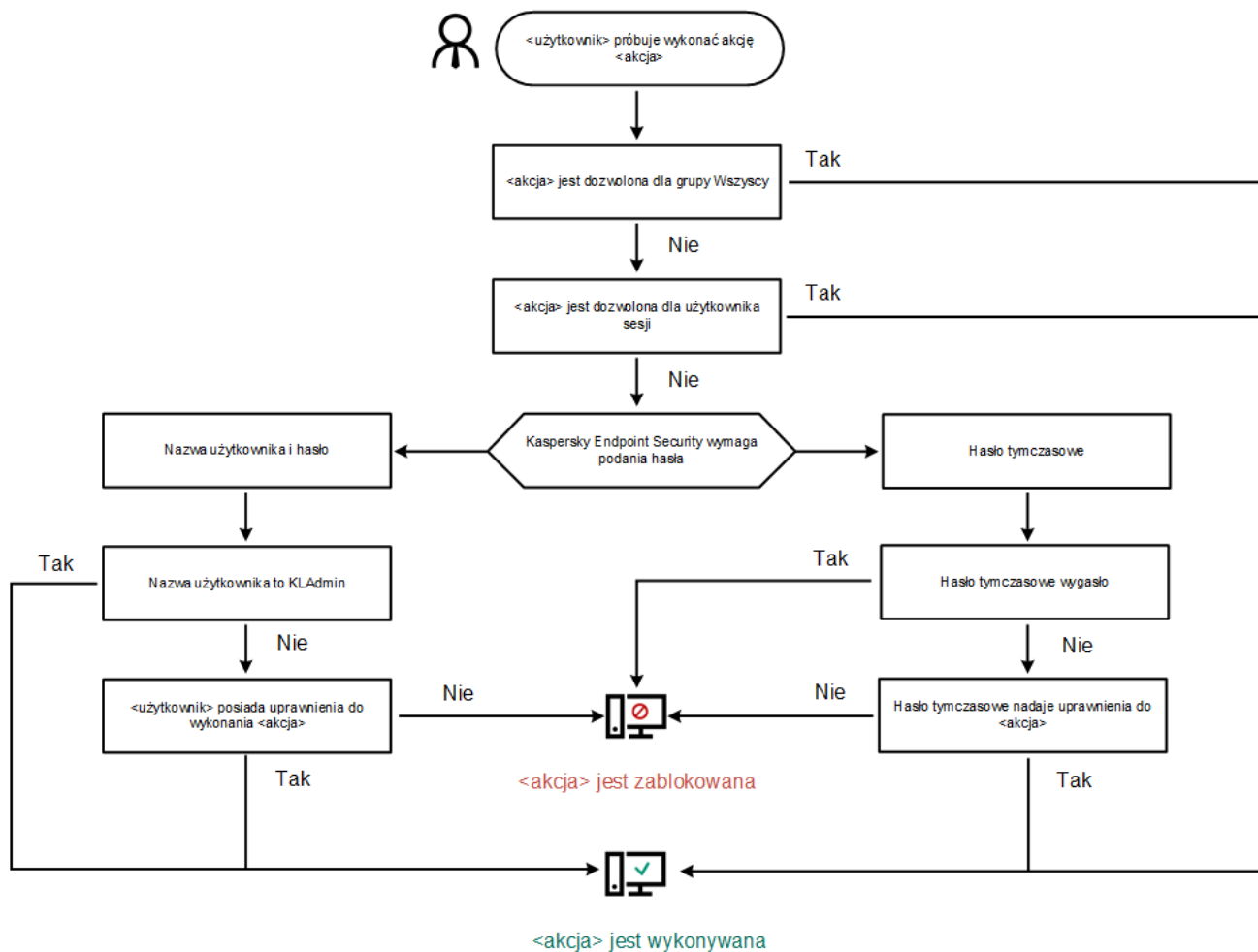
- **KLAdmin.** Konto administratora z nieograniczonym dostępem do Kaspersky Endpoint Security. Konto KLAdmin posiada prawo do wykonania dowolnego działania, które jest chronione hasłem. Uprawnień dla konta KLAdmin nie można wycofać. Jeśli włączysz ochronę hasłem, Kaspersky Endpoint Security wyświetli monit o ustawienie hasła dla konta KLAdmin.
- **Grupa Każda.** Wbudowana grupa Windows, która zawiera wszystkich użytkowników w obrębie sieci firmowej. Użytkownicy w grupie Każda mogą uzyskać dostęp do aplikacji zgodnie z uprawnieniami, które są im nadane.
- **Użytkownicy indywidualni lub grupy.** Konta użytkowników, dla których możesz skonfigurować uprawnienia indywidualne. Na przykład, jeśli działanie jest zablokowane dla grupy Każda, możesz zezwolić na to działanie dla użytkownika indywidualnego lub grupy.
- **Użytkownik sesji.** Konto użytkownika, który uruchomił sesję systemu Windows. Po wyświetleniu monitu o podanie hasła, możesz przełączyć się do innego użytkownika sesji (pole **Zapisz hasło dla bieżącej sesji**). W tym przypadku Kaspersky Endpoint Security odnosi się do użytkownika, którego dane uwierzytelniające zostały wprowadzone jako użytkownika sesji zamiast użytkownika, który rozpoczął sesję systemu Windows.

Hasło tymczasowe

Hasło tymczasowe może zostać użyte do nadania tymczasowego dostępu do Kaspersky Endpoint Security dla pojedynczego komputera poza siecią firmową. Administrator generuje hasło tymczasowe dla indywidualnego komputera we właściwościach komputera w Kaspersky Security Center. Administrator wybierz działania, które będą chronione hasłem tymczasowym, i określa okres ważności hasła tymczasowego.

Algorytm działania ochrony hasłem

Kaspersky Endpoint Security decyduje, czy zezwolić na lub zablokować działanie ochrony hasłem w oparciu o następujący algorytm (patrz rysunek poniżej).




Algorytm działania ochrony hasłem

Włączanie ochrony hasłem

Ochrona hasłem umożliwia ograniczenie dostępu użytkowników do Kaspersky Endpoint Security zgodnie z uprawnieniami im nadanymi (na przykład, uprawnienie do zakończenia działania aplikacji).

W celu włączenia ochrony hasłem:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Interfejs**.
3. Użyj przełącznika **Ochrona hasłem**, aby włączyć lub wyłączyć komponent.
4. Określ hasło dla konta KLAdmin i potwierdź je.

Konto KLAdmin posiada prawo do wykonania dowolnego działania, które jest chronione hasłem.

Jeśli komputer działa pod kontrolą profilu, Administrator może zresetować hasło dla konta KLAdmin we właściwościach profilu. Jeśli komputer nie jest połączony z Kaspersky Security Center, a Ty zapomniałeś hasło do konta KLAdmin, nie ma możliwości odzyskania hasła.

5. Ustaw uprawnienia dla wszystkich użytkowników w sieci firmowej:

a. W tabeli **Uprawnienia** kliknij przycisk **Edytuj**, aby otworzyć listę uprawnień dla grupy Każda.

Grupa Każda jest wbudowaną grupą Windows, która zawiera wszystkich użytkowników w obrębie sieci firmowej.

b. Zaznacz pola obok działań, które użytkownicy będą mogli wykonywać bez wprowadzenia hasła.

Jeśli pole jest odznaczone, użytkownicy nie mogą wykonywać tego działania. Na przykład, jeśli pole obok uprawnienia **Zakończenie działania aplikacji** jest odznaczone, możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako KLAdmin lub jako [pojedynczy użytkownik, który posiada wymagane uprawnienie](#), lub jeśli wprowadzisz [hasło tymczasowe](#).

Uprawnienia Ochrony hasłem obejmują pewne ważne [aspekty, które należy rozważyć](#). Upewnij się, że wszystkie warunki dla uzyskania dostępu do Kaspersky Endpoint Security zostaną spełnione.

c. Kliknij przycisk **OK**.

6. Zapisz swoje zmiany.

Jeśli ochrona hasłem jest włączona, aplikacja ograniczy dostęp użytkowników do Kaspersky Endpoint Security zgodnie z uprawnieniami nadanymi grupie Każda. Możesz wykonać działania, które są zablokowane dla grupy Każda tylko wtedy, gdy korzystasz z konta KLAdmin, [innego konta posiadającego wymagane uprawnienia](#), lub jeśli wprowadzasz [hasło tymczasowe](#).

Możesz wyłączyć Ochronę hasłem tylko wtedy, gdy jesteś zalogowany jako KLAdmin. Nie można wyłączyć ochrony hasłem, jeśli używasz innego konta użytkownika lub hasła tymczasowego.


Podczas sprawdzania hasła możesz zaznaczyć pole **Zapisz hasło dla bieżącej sesji**. W tym przypadku Kaspersky Endpoint Security nie wyświetli monitu o podanie hasła, gdy użytkownik próbuje wykonać inne działanie ochrony hasłem na czas trwania sesji.

Nadawanie uprawnień pojedynczym użytkownikom lub grupom

Możesz udzielić dostępu do Kaspersky Endpoint Security pojedynczym użytkownikom lub grupom. Na przykład, jeśli istniejąca aplikacja jest zablokowana dla grupy Każda, możesz nadać uprawnienie **Zakończenie działania aplikacji** pojedynczemu użytkownikowi. W wyniku tego możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako ten użytkownik lub jako KLAdmin.

Możesz użyć danych uwierzytelniających do konta, aby uzyskać dostęp do aplikacji tylko wtedy, gdy komputer jest w domenie. Jeśli komputer nie znajduje się w domenie, możesz użyć konta KLAdmin lub [hasła tymczasowego](#).

W celu nadania uprawnień pojedynczym użytkownikom lub grupom:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Interfejs**.
3. W tabeli **Ochrona hasłem** kliknij przycisk **Dodaj**.
4. W otwartym oknie kliknij przycisk **Wybierz użytkownika lub grupę**.

Zostanie otwarte standardowe okno Wybierz Użytkowników lub Grupy.

- Wybierz użytkownika lub grupę w Active Directory i potwierdź swój wybór.
- Na liście **Uprawnienia** zaznacz pola obok działań, które wybrany użytkownik lub grupa będą mogli wykonywać bez pytania o podanie hasła.

Jeśli pole jest odznaczone, użytkownicy nie mogą wykonywać tego działania. Na przykład, jeśli pole obok uprawnienia **Zakończenie działania aplikacji** jest odznaczone, możesz zakończyć działanie aplikacji tylko wtedy, gdy jesteś zalogowany jako KLAdmin lub jako [pojedynczy użytkownik, który posiada wymagane uprawnienie](#), lub jeśli wprowadzisz [hasło tymczasowe](#).

Uprawnienia Ochrony hasłem obejmują pewne ważne [aspekty, które należy rozważyć](#). Upewnij się, że wszystkie warunki dla uzyskania dostępu do Kaspersky Endpoint Security zostaną spełnione.

- Zapisz swoje zmiany.

W wyniku tego działania, jeśli dostęp do aplikacji zostanie ograniczony dla grupy Każda, użytkownicy będą mieli uprawnienia dostępu do Kaspersky Endpoint Security zgodnie z pojedynczymi uprawnieniami użytkowników.

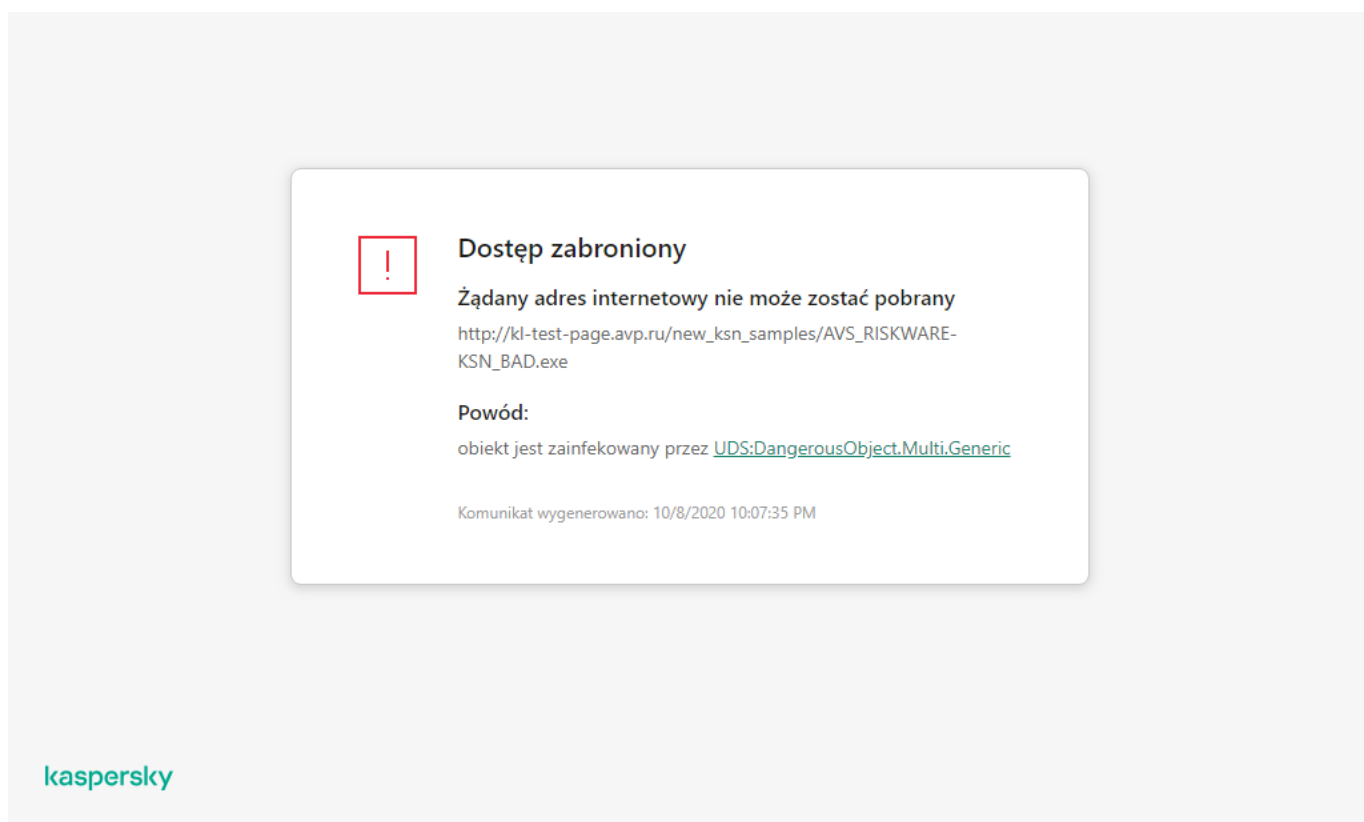
Używanie hasła tymczasowego do nadawania uprawnień

Hasło tymczasowe może zostać użyte do nadania tymczasowego dostępu do Kaspersky Endpoint Security dla pojedynczego komputera poza siecią firmową. Jest to konieczne do zezwolenia użytkownikowi na wykonanie zablokowanego działania bez uzyskania danych uwierzytelniających konta KLAdmin. Aby użyć hasła tymczasowego, komputer musi zostać dodany do Kaspersky Security Center.

W celu zezwolenia użytkownikowi na wykonanie zablokowanego działania, korzystając z hasła tymczasowego:

- Otwórz Konsolę administracyjną Kaspersky Security Center.
- W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
- W obszarze roboczym wybierz zakładkę **Urządzenia**.
- Kliknij dwukrotnie komputer, aby otworzyć okno właściwości komputera.
- W oknie ustawień komputera wybierz sekcję **Aplikacje**.
- Na liście aplikacji Kaspersky zainstalowanych na komputerze wybierz **Kaspersky Endpoint Security for Windows** i kliknij ją dwukrotnie, aby otworzyć właściwości aplikacji.
- W oknie ustawień aplikacji wybierz **Ustawienia główne** → **Interfejs**.
- W sekcji **Ochrona hasłem** kliknij przycisk **Ustawienia**.
Zostanie otwarte okno **Ochrona hasłem**.
- W sekcji **Hasło tymczasowe** kliknij przycisk **Ustawienia**.
Zostanie otwarte okno **Utwórz hasło tymczasowe**.
- W polu **Data wygaśnięcia** określ datę wygaśnięcia hasła tymczasowego.

11. W tabeli **Zakres hasła tymczasowego** zaznacz pola obok działań, które będą dostępne dla użytkownika po wprowadzeniu hasła tymczasowego.
12. Kliknij przycisk **Utwórz**.
Zostanie otwarte okno zawierające hasło tymczasowe (patrz rysunek poniżej).
13. Skopiuj hasło i dostarcz je użytkownikowi.




Hasło tymczasowe

Specjalne kwestie dotyczące uprawnień Ochrony hasłem

Uprawnienia Ochrony hasłem obejmują pewne ważne aspekty i ograniczenia, które należy rozważyć.

Ustawienia aplikacji

Jeśli komputer użytkownika działa pod kontrolą profilu, upewnij się, że wszystkie wymagane ustawienia w profilu są dostępne do edycji (atributy  są otwarte).


Zakończenie działania aplikacji

Nie ma żadnych specjalnych kwestii ani ograniczeń.


Wyłączenie składników ochrony

- Nie można przyznać uprawnień do wyłączenia składników ochrony dla grupy Wszyscy. Aby zezwolić użytkownikom innym niż KLAdmin na wyłączenie składników ochrony, [dodaj użytkownika lub grupę](#), który/która

posiada uprawnienie **Wyłącz składniki ochrony** w ustawieniach Ochrony hasłem.

- Jeśli komputer użytkownika działa pod kontrolą profilu, upewnij się, że wszystkie wymagane ustawienia w profilu są dostępne do edycji (atrybuty  są otwarte).
- Aby wyłączyć składniki ochrony w ustawieniach aplikacji, użytkownik musi mieć uprawnienie **Konfiguracja ustawień aplikacji**.
- Aby wyłączyć składniki ochrony z poziomu menu kontekstowego (korzystając z elementu menu **Wstrzymaj ochronę**), użytkownik musi mieć uprawnienie **Wyłączenie składników kontroli** jako dodatek do uprawnienia **Wyłączenie składników ochrony**.

Wyłączenie składników kontroli

- Nie można przyznać uprawnienia do wyłączenia składników kontroli dla grupy Wszyscy. Aby zezwolić użytkownikom innym niż KLAdmin na wyłączenie składników kontroli, [dodaj użytkownika lub grupę](#), który/która posiada uprawnienie **Wyłącz składniki kontroli** w ustawieniach Ochrony hasłem.
- Jeśli komputer użytkownika działa pod kontrolą profilu, upewnij się, że wszystkie wymagane ustawienia w profilu są dostępne do edycji (atrybuty  są otwarte).
- Aby wyłączyć składniki kontroli w ustawieniach aplikacji, użytkownik musi mieć uprawnienie **Konfiguracja ustawień aplikacji**.
- Aby wyłączyć składniki kontroli z poziomu menu kontekstowego (korzystając z elementu menu **Wstrzymaj ochronę**), użytkownik musi mieć uprawnienie **Wyłączenie składników ochrony** jako dodatek do uprawnienia **Wyłączenie składników kontroli**.

Wyłączenie zasady Kaspersky Security Center

Nie możesz udzielić grupie „Wszyscy” uprawnienia do wyłączenia profilu Kaspersky Security Center. Aby zezwolić użytkownikom innym niż KLAdmin na wyłączenie profilu, [dodaj użytkownika lub grupę](#), który/która posiada uprawnienie **Wyłączenie zasady Kaspersky Security Center** w ustawieniach Ochrony hasłem.

Usuwanie klucza

Nie ma żadnych specjalnych kwestii ani ograniczeń.

Deinstalacja / modyfikacja / przywracanie aplikacji

Jeśli posiadasz dozwolone usuwanie, modyfikowanie i przywracanie aplikacji dla grupy „Wszystkie”, Kaspersky Endpoint Security nie wymaga podania hasła podczas próby wykonania tych działań przez użytkownika. Dlatego każdy użytkownik, także użytkownicy spoza domeny, może zainstalować, zmodyfikować lub przywrócić aplikację.

Przywracanie dostępu do danych na zaszyfrowanych dyskach

Możesz odzyskać dostęp do danych na zaszyfrowanych dyskach tylko wtedy, gdy jesteś zalogowany jako KLAdmin. Uprawnienie do wykonywania tego działania nie może zostać nadane żadnemu innemu użytkownikowi.

Wyświetlanie raportów

Nie ma żadnych specjalnych kwestii ani ograniczeń.

Przywróć z Kopii zapasowej

Nie ma żadnych specjalnych kwestii ani ograniczeń.

Strefa zaufana

Strefa zaufana jest utworzoną przez administratora listą obiektów i aplikacji, które nie są monitorowane przez Kaspersky Endpoint Security.

Administrator tworzy strefę zaufaną, biorąc pod uwagę cechy i funkcje używanych obiektów oraz zainstalowanych aplikacji. Umieszczenie obiektów i aplikacji w strefie zaufanej może być konieczne, gdy Kaspersky Endpoint Security blokuje dostęp do określonego obiektu lub aplikacji, które według Ciebie są nieszkodliwe. Administrator może także zezwolić użytkownikowi na utworzenie własnej lokalnej strefy zaufanej dla określonego komputera. W ten sposób użytkownicy mogą utworzyć swoje własne lokalne listy wykluczeń i zaufanych aplikacji jako dodatek do ogólnej strefy zaufanej w zasadzie.

Tworzenie wykluczenia ze skanowania

Wykluczenie ze skanowania to zestaw warunków, które muszą być spełnione, aby Kaspersky Endpoint Security nie skanował określonego obiektu w poszukiwaniu wirusów i innych zagrożeń.

Wykluczenia ze skanowania zapewniają możliwość bezpiecznej pracy z legalnymi aplikacjami, które mogą zostać wykorzystane przez hakerów do uszkodzenia komputera lub danych. Nie posiadają one żadnych szkodliwych funkcji, ale mogą zostać wykorzystane przez cyberprzestępców. Szczegółowe informacje o legalnym oprogramowaniu, które może zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych osobistych użytkownika, znajdują się na [stronie internetowej Encyklopedii IT Kaspersky](#).

Takie aplikacje mogą być blokowane przez program Kaspersky Endpoint Security. Aby zapobiec blokowaniu tych aplikacji, możesz skonfigurować wykluczenia ze skanowania dla używanych aplikacji. W tym celu dodaj do strefy zaufanej nazwę lub maskę nazwy zgodną z klasyfikacją Encyklopedii IT Kaspersky. Na przykład, często używasz aplikacji Radmin do zdalnego zarządzania komputerami. Kaspersky Endpoint Security wykrywa ten rodzaj aktywności aplikacji jako podejrzany i może go zablokować. Aby zapobiec blokowaniu aplikacji, utwórz wykluczenie ze skanowania z nazwą lub maską nazwy z Encyklopedii IT Kaspersky.

Jeśli na komputerze jest zainstalowana aplikacja, która gromadzi informacje i wysyła je do przetworzenia, Kaspersky Endpoint Security może zaklasyfikować tę aplikację jako szkodliwe oprogramowanie. Aby tego uniknąć, możesz wykluczyć tę aplikację ze skanowania, konfigurując Kaspersky Endpoint Security w sposób opisany w dokumencie.

Wykluczenia ze skanowania mogą być używane przez następujące komponenty i zadania aplikacji, które zostały skonfigurowane przez administratora systemu:

- [Wykrywanie zachowań](#).
- [Ochrona przed exploitami](#).
- [Ochrona przed włamaniami](#).
- [Ochrona plików](#).
- [Ochrona WWW](#).
- [Ochrona poczty](#).
- [Zadania skanowania](#).

Kaspersky Endpoint Security nie przeskanuje obiektu, jeśli dysk lub folder go zawierający znajduje się w obszarze skanowania w momencie uruchomienia jednego z zadań skanowania. Wykluczenie ze skanowania nie jest stosowane, gdy dla danego obiektu uruchomione zostało skanowanie obiektów.

[Jak utworzyć wykluczenie ze skanowania w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Ustawienia główne** → **Wykluczenia**.
6. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** kliknij przycisk **Ustawienia**.
7. W oknie **Strefa zaufana** przejdź na zakładkę **Wykluczenia ze skanowania**.
Zostanie otwarte okno zawierające listę wykluczeń.
8. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę wykluczeń dla wszystkich komputerów w firmie. Listy wykluczeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Wykluczenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie wykluczeń zasady nadrzędnej nie jest możliwe.
9. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy wykluczeń, zaznacz pole **Zezwól na korzystanie z lokalnych wykluczeń**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę wykluczeń jako dodatek do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Jeśli lokalna lista została wygenerowana, po wyłączeniu tej funkcjonalności program Kaspersky Endpoint Security kontynuuje wykluczenie listy plików ze skanowania.
10. Kliknij przycisk **Dodaj**.
11. W celu wykluczenia pliku lub folderu ze skanowania:
 - a. W sekcji **Właściwości** zaznacz pole **Plik lub folder**.
 - b. Kliknij odnośnik **wybierz plik lub folder** w sekcji **Opis wykluczenia ze skanowania**, aby otworzyć okno **Nazwa pliku lub folderu**.
 - c. Wprowadź nazwę pliku lub folderu bądź maskę nazwy pliku lub folderu, albo wybierz plik lub folder w drzewie folderów, klikając **Przełóżaj**.

Użyj masek:

- Znak ***** (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:**.txt** będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
- Dwa występujące po sobie znaki ****** zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:\Folder***.txt** będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie **Folder** i w jego podfolderach. Maskę musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maskę **C:***.txt** nie jest ważną maską.

- Znak **?** (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:\Folder\???.txt** będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie **Folder**, które posiadają rozszerzenie **TXT** i nazwę składającą się z trzech znaków.

d. W oknie **Nazwa pliku lub folderu** kliknij **OK**.

Odnośnik do dodanego pliku lub folderu pojawi się w oknie **Wykluczenie ze skanowania**, w sekcji **Opis wykluczenia ze skanowania**.

12. W celu wykluczenia obiektów o określonej nazwie ze skanowania:

a. W sekcji **Właściwości** zaznacz pole **Nazwa obiektu**.

b. Kliknij odnośnik **wprowadź nazwę obiektu** w sekcji **Opis wykluczenia ze skanowania**, aby otworzyć okno **Nazwa obiektu**.

c. Wprowadź nazwę typu obiektu zgodnie z klasyfikacją [Encyklopedii Kaspersky](#) (na przykład: **Email-Worm**, **Rootkit** lub **RemoteAdmin**).

Możesz użyć masek ze znakiem **?** (zastępuje dowolny pojedynczy znak) oraz znak ***** (zastępuje dowolną liczbę znaków). Na przykład, jeśli określona jest maska **Client***, Kaspersky Endpoint Security wyklucza obiekty **Client-IRC**, **Client-P2P** i **Client-SMTP** ze skanowania.

d. Kliknij przycisk **OK** w oknie **Nazwa obiektu**.

Odnośnik do dodanej nazwy obiektu pojawi się w oknie **Wykluczenie ze skanowania**, w sekcji **Opis wykluczenia ze skanowania**.

13. Jeśli chcesz wykluczyć pojedynczy plik ze skanowania:

a. W sekcji **Właściwości** zaznacz pole **Suma kontrolna obiektu**.

b. Kliknij odnośnik wpisu sumy kontrolnej obiektu, aby otworzyć okno **Suma kontrolna obiektu**.

c. Wprowadź sumę kontrolną pliku lub wybierz plik, klikając przycisk **Przeglądaj**.

Jeśli plik został zmodyfikowany, suma kontrolna pliku także zostanie zmodyfikowana. Jeśli taka sytuacja będzie miała miejsce, zmodyfikowany plik nie zostanie dodany do wykluczeń.

d. Kliknij **OK** w oknie **Suma kontrolna obiektu**.

Odnośnik do dodanego obiektu pojawi się w oknie **Wykluczenie ze skanowania**, w sekcji **Opis wykluczenia ze skanowania**.

14. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

15. Wskaż moduły programu Kaspersky Endpoint Security, które będą używać wykluczenia ze skanowania:

a. Po kliknięciu odnośnika **dowolne** w sekcji **Opis wykluczenia ze skanowania**, zostanie aktywowany odnośnik **wybierz moduły**.

b. Kliknięcie odnośnika **wybierz moduły** otwiera okno **Składniki ochrony**.

c. Zaznacz pola obok komponentów, do których mają być stosowane wykluczenia ze skanowania.

d. W oknie **Składniki ochrony** kliknij **OK**.

W przypadku określenia komponentów w ustawieniach wykluczenia ze skanowania, to wykluczenie będzie stosowane tylko podczas skanowania przez te moduły programu Kaspersky Endpoint Security.

W przypadku, gdy komponenty nie zostaną określone w ustawieniach wykluczenia ze skanowania, to wykluczenie będzie stosowane podczas skanowania przez wszystkie moduły programu Kaspersky Endpoint Security.

16. W dowolnym momencie możesz użyć pola do [zatrzymania wykluczenia](#).

17. Zapisz swoje zmiany.

[Jak utworzyć wykluczenie ze skanowania w Web Console i Cloud Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz dodać wykluczenie. Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia główne** → **Wykluczenia**.
5. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** kliknij odnośnik **Wykluczenia ze skanowania**.
6. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę wykluczeń dla wszystkich komputerów w firmie. Listy wykluczeń w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Wykluczenia z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie wykluczeń zasady nadrzędnej nie jest możliwe.
7. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy wykluczeń, zaznacz pole **Zezwól na korzystanie z lokalnych wykluczeń**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę wykluczeń jako dodatek do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy wykluczeń, wygenerowanej w zasadzie. Jeśli lokalna lista została wygenerowana, po wyłączeniu tej funkcjonalności program Kaspersky Endpoint Security kontynuuje wykluczenie listy plików ze skanowania.
8. Kliknij przycisk **Dodaj**.
9. Wybierz sposób dodania wykluczenia: **Plik lub folder**, **Nazwa obiektu** lub **Suma kontrolna obiektu**.
10. Jeśli chcesz wykluczyć plik lub folder ze skanowania, wybierz plik lub folder, klikając przycisk **Przełóżnik**.
Możesz również ręcznie wprowadzić ścieżkę. Kaspersky Endpoint Security obsługuje znaki * i ? podczas wprowadzania maski:
 - Znak * (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:**.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
 - Dwa występujące po sobie znaki * zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder***.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie Folder i w jego podfolderach. Maskę musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maskę C:***.txt nie jest ważną maską.
 - Znak ? (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder\???.txt będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie Folder, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.
11. Jeśli chcesz wykluczyć określony typ obiektu ze skanowania, w polu **Obiekt** wprowadź nazwę typu obiektu zgodnie z klasyfikacją [Encyklopedii Kaspersky](#) (na przykład: Email-Worm, Rootkit lub RemoteAdmin).

Możesz użyć masek ze znakiem `?` (zastępuje dowolny pojedynczy znak) oraz znak `*` (zastępuje dowolną liczbę znaków). Na przykład, jeśli określona jest maska `Client*`, Kaspersky Endpoint Security wyklucza obiekty `Client-IRC`, `Client-P2P` i `Client-SMTP` ze skanowania.

12. Jeśli chcesz wykluczyć pojedynczy plik ze skanowania, wprowadź sumę kontrolną pliku w polu **Suma kontrolna pliku**.

Jeśli plik został zmodyfikowany, suma kontrolna pliku także zostanie zmodyfikowana. Jeśli taka sytuacja będzie miała miejsce, zmodyfikowany plik nie zostanie dodany do wykluczeń.


13. W sekcji **Składniki ochrony** wybierz komponenty, do których ma zostać zastosowane wykluczenie ze skanowania.

14. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.

15. W dowolnym momencie możesz użyć przełącznika do [zatrzymania wykluczenia](#).

16. Zapisz swoje zmiany.

[Jak utworzyć wykluczenie ze skanowania w interfejsie aplikacji?](#) 

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Zagrożenia i wykluczenia**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Zarządzaj wykluczeniami**.
4. Kliknij przycisk **Dodaj**.
5. Jeśli chcesz wykluczyć plik lub folder ze skanowania, wybierz plik lub folder, klikając przycisk **Przeglądaj**.
Możesz również ręcznie wprowadzić ścieżkę. Kaspersky Endpoint Security obsługuje znaki * i ? podczas wprowadzania maski:
 - Znak * (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:**.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
 - Dwa występujące po sobie znaki * zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder***.txt będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie Folder i w jego podfolderach. Maskę musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maskę C:***.txt nie jest ważną maską.
 - Znak ? (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: \ i / (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska C:\Folder\???.txt będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie Folder, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.
6. Jeśli chcesz wykluczyć określony typ obiektu ze skanowania, w polu **Obiekt** wprowadź nazwę typu obiektu zgodnie z klasyfikacją [Encyklopedii Kaspersky](#) (na przykład: Email-Worm, Rootkit lub RemoteAdmin).
Możesz użyć masek ze znakiem ? (zastępuje dowolny pojedynczy znak) oraz znak * (zastępuje dowolną liczbę znaków). Na przykład, jeśli określona jest maska Client*, Kaspersky Endpoint Security wyklucza obiekty Client-IRC, Client-P2P i Client-SMTP ze skanowania.
7. Jeśli chcesz wykluczyć pojedynczy plik ze skanowania, wprowadź sumę kontrolną pliku w polu **Suma kontrolna pliku**.
Jeśli plik został zmodyfikowany, suma kontrolna pliku także zostanie zmodyfikowana. Jeśli taka sytuacja będzie miała miejsce, zmodyfikowany plik nie zostanie dodany do wykluczeń.
8. W sekcji **Składniki ochrony** wybierz komponenty, do których ma zostać zastosowane wykluczenie ze skanowania.
9. Jeśli to konieczne, w polu **Komentarz** wprowadź krótki komentarz dotyczący tworzonego wykluczenia ze skanowania.
10. Dla wykluczenia wybierz stan **Aktywny**.
W dowolnym momencie możesz użyć przełącznika do [zatrzymania wykluczenia](#).
11. Zapisz swoje zmiany.

Przykłady masek ścieżek:

Ścieżki do plików znajdujących się w dowolnym folderze:

- Maska `*.exe` będzie zawierała wszystkie ścieżki do plików, które posiadają rozszerzenie exe.
- Maski `example*` będzie zawierała wszystkie ścieżki do plików o nazwie EXAMPLE.

Ścieżki do plików znajdujących się w określonym folderze:


- Maski `C:\dir*.*` będzie zawierała wszystkie ścieżki do plików znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
- Maski `C:\dir\` będzie zawierała wszystkie ścieżki do plików znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
- Maski `C:\dir\` będzie zawierała wszystkie ścieżki do plików znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
- Maski `C:\dir*.exe` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem EXE, znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
- Maski `C:\dir\test` będzie zawierała wszystkie ścieżki do plików o nazwie „test” znajdujących się w folderze C:\dir\, ale nie w podfolderach C:\dir\.
- Maski `C:\dir*\test` będzie zawierała wszystkie ścieżki do plików o nazwie „test” znajdujących się w folderze C:\dir\ i w podfolderach C:\dir\.

Ścieżki do plików znajdujących się we wszystkich folderach z określoną nazwą:

- Maski `dir*.*` będzie zawierała wszystkie ścieżki do plików w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.
- Maski `dir*` będzie zawierała wszystkie ścieżki do plików w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.
- Maski `dir\` będzie zawierała wszystkie ścieżki do plików w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.
- Maski `dir*.exe` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem EXE, znajdujących się w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.
- Maski `dir\test` będzie zawierała wszystkie ścieżki do plików o nazwie „test”, znajdujących się w folderach o nazwie „dir”, ale nie w podfolderach tych folderów.

Włączanie i wyłączanie wykluczenia ze skanowania

W celu włączenia lub wyłączenia wykluczenia ze skanowania:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Zagrożenia i wykluczenia**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Zarządzaj wykluczeniami**.
4. Na liście wykluczeń ze skanowania wybierz żądane wykluczenie.

5. Użyj przełącznika obok obiektu, aby włączyć ten obiekt do obszaru skanowania lub żeby go wyłączyć.

6. Zapisz swoje zmiany.

Modyfikowanie listy zaufanych aplikacji

Lista zaufanych aplikacji jest listą aplikacji, których aktywność sieciowa i plikowa (włączając w to szkodliwą aktywność) oraz dostęp do rejestru systemowego nie są monitorowane przez Kaspersky Endpoint Security. Domyślnie program Kaspersky Endpoint Security skanuje obiekty otwierane, uruchamiane lub zapisywane przez proces dowolnej aplikacji i monitoruje aktywność wszystkich aplikacji oraz ruch sieciowy będący wynikiem ich działania. Jednakże aplikacja, która została dodana do listy zaufanych aplikacji zostanie wykluczona ze skanowań wykonywanych przez Kaspersky Endpoint Security.

Jeżeli uważasz, że obiekty używane przez Notatnik firmy Microsoft Windows są nieszkodliwe i nie wymagają skanowania, dodaj Notatnik firmy Microsoft Windows do listy zaufanych aplikacji. Podczas skanowania pomijane będą obiekty używane przez ten program.

Oprócz tego pewne akcje zaklasyfikowane przez Kaspersky Endpoint Security jako podejrzane mogą być traktowane przez inne aplikacje jako nieszkodliwe. Na przykład przechwytywanie danych wprowadzanych z klawiatury jest charakterystyczne dla aplikacji, które automatycznie przełączają układ klawiatury (np. Punto Switcher). Aby korzystać z właściwości takich aplikacji i wyłączyć monitorowanie ich aktywności, dodaj je do listy zaufanych aplikacji.

Wykluczenie zaufanych aplikacji ze skanowania pozwala uniknąć problemów kompatybilności Kaspersky Endpoint Security z innymi programami (np. problem podwójnego skanowania ruchu sieciowego przez Kaspersky Endpoint Security i przez inną aplikację antywirusową), jak również zwiększyć wydajność komputera, która w niektórych sytuacjach osiąga wartość krytyczną.

Należy pamiętać, że pliki wykonywalne oraz procesy zaufanych aplikacji będą nadal skanowane w poszukiwaniu wirusów i szkodliwych programów. Aplikacja może zostać całkowicie wykluczona ze skanowania wykonywanego przez program Kaspersky Endpoint Security przy użyciu wykluczeń ze skanowania.

[Dodawanie aplikacji do listy zaufanych w Konsoli administracyjnej \(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Ustawienia główne** → **Wykluczenia**.
6. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** kliknij przycisk **Ustawienia**.
7. W oknie **Strefa zaufana** przejdź na zakładkę **Zaufane aplikacje**.
Zostanie otwarte okno zawierające listę zaufanych aplikacji.
8. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę zaufanych aplikacji dla wszystkich komputerów w firmie. Listy zaufanych aplikacji w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Zaufane aplikacje z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie zaufanych aplikacji zasady nadrzędnej nie jest możliwe.
9. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy zaufanych aplikacji, zaznacz pole **Zezwól na korzystanie z lokalnych zaufanych aplikacji**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę zaufanych aplikacji jako dodatek do ogólnej listy zaufanych aplikacji, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy zaufanych aplikacji, wygenerowanej w zasadzie. Jeśli lokalna lista została wygenerowana, po wyłączeniu tej funkcjonalności program Kaspersky Endpoint Security kontynuuje wykluczenie listy zaufanych aplikacji ze skanowania.
10. Kliknij przycisk **Dodaj**.
11. W otwartym oknie wprowadź ścieżkę do pliku wykonywalnego zaufanej aplikacji.
Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki ***** i **?**.

Kaspersky Endpoint Security nie obsługuje zmiennej środowiskowej %userprofile% podczas generowania listy zaufanych aplikacji w konsoli Kaspersky Security Center. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku * (na przykład: C:\Users*\Documents\File.exe).


Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.
12. Skonfiguruj zaawansowane ustawienia zaufanej aplikacji (zapoznaj się z poniższą tabelą).
13. W dowolnym momencie możesz użyć pola do [wykluczenia aplikacji z zaufanej strefy](#).
14. Zapisz swoje zmiany.

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz dodać aplikację do listy zaufanych.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia główne** → **Wykluczenia**.
5. W sekcji **Wykluczenia ze skanowania i aplikacje zaufane** kliknij odnośnik **Zaufane aplikacje**.
Zostanie otwarte okno zawierające listę zaufanych aplikacji.
6. Zaznacz pole **Przenieś wartości podczas dziedziczenia**, jeśli chcesz utworzyć skonsolidowaną listę zaufanych aplikacji dla wszystkich komputerów w firmie. Listy zaufanych aplikacji w zasadach nadrzędnych i podrzędnych zostaną scalone. Listy zostaną scalone pod warunkiem, że scalone wartości podczas dziedziczenia są włączone. Zaufane aplikacje z zasady nadrzędnej są wyświetlane w zasadach podrzędnych w widoku tylko do odczytu. Zmiana lub usunięcie zaufanych aplikacji zasady nadrzędnej nie jest możliwe.
7. Jeśli chcesz umożliwić użytkownikowi utworzenie lokalnej listy zaufanych aplikacji, zaznacz pole **Zezwól na korzystanie z lokalnych zaufanych aplikacji**. W ten sposób użytkownik może utworzyć swoją własną lokalną listę zaufanych aplikacji jako dodatek do ogólnej listy zaufanych aplikacji, wygenerowanej w zasadzie. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.

Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnej listy zaufanych aplikacji, wygenerowanej w zasadzie. Jeśli lokalna lista została wygenerowana, po wyłączeniu tej funkcjonalności program Kaspersky Endpoint Security kontynuuje wykluczenie listy zaufanych aplikacji ze skanowania.
8. Kliknij przycisk **Dodaj**.
9. W otwartym oknie wprowadź ścieżkę do pliku wykonywalnego zaufanej aplikacji.
Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki ***** i **?**.

Kaspersky Endpoint Security nie obsługuje zmiennej środowiskowej %userprofile% podczas generowania listy zaufanych aplikacji w konsoli Kaspersky Security Center. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku * (na przykład: C:\Users*\Documents\File.exe).

Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.
10. Skonfiguruj zaawansowane ustawienia zaufanej aplikacji (zapoznaj się z poniższą tabelą).
11. W dowolnym momencie możesz użyć pola do [wykluczenia aplikacji z zaufanej strefy](#).
12. Zapisz swoje zmiany.

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Zagrożenia i wykluczenia**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Określ zaufane aplikacje**.
4. W oknie kliknij przycisk **Dodaj**.
5. Wybierz plik wykonywalny zaufanej aplikacji.

Możesz również ręcznie wprowadzić ścieżkę. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki * i ?.

Kaspersky Endpoint Security obsługuje zmienne środowiskowe i konwertuje ścieżkę w lokalnym interfejsie aplikacji. Innymi słowy, jeśli wprowadzisz ścieżkę do pliku %userprofile%\Documents\File.exe, w lokalnym interfejsie aplikacji dla użytkownika Fred123 dodaj wpis C:\Users\Fred123\Documents\File.exe. Zgodnie z tym ustawieniem, program Kaspersky Endpoint Security ignoruje zaufany program File.exe dla innych użytkowników. Aby zastosować wpis do wszystkich kont użytkowników, możesz użyć znaku * (na przykład: C:\Users*\Documents\File.exe).

Za każdym razem, gdy dodajesz nową zmienną środowiskową, musisz uruchomić aplikację ponownie.

6. W oknie właściwości zaufanej aplikacji skonfiguruj ustawienia zaawansowane (patrz poniższa tabela).
7. W dowolnym momencie możesz użyć pola do [wykluczenia aplikacji z zaufanej strefy](#).
8. Zapisz swoje zmiany.


Ustawienia zaufanej aplikacji

Parametr	Opis
Nie skanuj otwieranych plików	Wszystkie pliki, które są otwierane przez aplikację, zostają wykluczone ze skanowania wykonywanego przez program Kaspersky Endpoint Security. Na przykład, jeśli używasz aplikacji do tworzenia kopii zapasowej plików, ta funkcja pomaga w zmniejszeniu zużycia zasobów przez Kaspersky Endpoint Security.
Nie monitoruj aktywności aplikacji	Kaspersky Endpoint Security nie będzie monitorował aktywności sieciowej i plikowej aplikacji w systemie operacyjnym. Aktywność aplikacji jest monitorowana przez następujące komponenty: Wykrywanie zachowań , Ochrona przed exploitami , Ochrona przed włamaniami , Silnik korygujący i Zapora sieciowa .
Nie dziedzicz ograniczeń nadrzędnego procesu (aplikacji)	Ograniczenia skonfigurowane dla procesu nadrzędnego nie będą stosowane przez program Kaspersky Endpoint Security do procesu podrzędnego. Proces nadrzędny jest uruchamiany przez aplikację, dla której skonfigurowano uprawnienia aplikacji (Ochrona przed włamaniami) i reguły sieciowe dla aplikacji (Zapora sieciowa).
Nie monitoruj aktywności aplikacji potomnych	Kaspersky Endpoint Security nie będzie monitorował aktywności plikowej i sieciowej aplikacji, które są uruchamiane przez tę aplikację.
Zezwól na	Autoochrona Kaspersky Endpoint Security blokuje wszystkie próby zarządzania usługami

interakcję z interfejsem aplikacji	aplikacji ze zdalnego komputera. Jeśli pole jest zaznaczone, aplikacja do zdalnej administracji może zarządzać ustawieniami Kaspersky Endpoint Security poprzez interfejs Kaspersky Endpoint Security.
Nie blokuj interakcji z modułem Ochrona AMSI <i>(dostępny tylko w Kaspersky Security Center Console)</i>	Kaspersky Endpoint Security nie będzie monitorował żądań zaufanej aplikacji dla obiektów skanowanych przez składnik Ochrona AMSI .
Nie skanuj ruchu sieciowego	Ruch sieciowy zainicjowany przez aplikację zostanie wykluczony ze skanowania wykonywanego przez Kaspersky Endpoint Security. Ze skanowania można wykluczyć cały ruch sieciowy lub tylko zaszyfrowany ruch sieciowy. Ze skanowania możesz także wykluczyć pojedyncze adresy IP i numery portów.
Komentarz	Jeśli to konieczne, możesz wpisać krótki komentarz dla zaufanej aplikacji. Komentarze pomagają uprościć wyszukiwanie i sortowanie zaufanych aplikacji.
Stan	Stan zaufanej aplikacji: <ul style="list-style-type: none"> • Stan Aktywny oznacza, że aplikacja znajduje się w strefie zaufanej. • Stan Nieaktywny oznacza, że aplikacja zostanie wykluczona ze strefy zaufanej.

Włączanie i wyłączanie reguł strefy zaufanej dla aplikacji na liście zaufanych aplikacji


W celu włączenia lub wyłączenia działania reguł strefy zaufanej stosowanych do aplikacji z listy zaufanych aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Zagrożenia i wykluczenia**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Określ zaufane aplikacje**.
4. Z listy zaufanych aplikacji wybierz odpowiednią aplikację.
5. Użyj przełącznika w kolumnie **Stan**, aby włączyć zaufaną aplikację do obszaru skanowania lub ją wykluczyć.
6. Zapisz swoje zmiany.

Korzystanie z magazynu zaufanych certyfikatów systemowych

Korzystanie z magazynu zaufanych certyfikatów systemowych umożliwia wykluczenie aplikacji posiadających zaufany podpis cyfrowy ze skanowań antywirusowych. Kaspersky Endpoint Security automatycznie przypisze takie aplikacje do grupy *Zaufane*.

W celu rozpoczęcia korzystania z magazynu zaufanych certyfikatów systemowych:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Zagrożenia i wykluczenia**.
3. Z listy rozwijalnej **Magazyn zaufanych certyfikatów systemowych** wybierz, który magazyn systemowy ma być uznawany za zaufany przez Kaspersky Endpoint Security.
4. Zapisz swoje zmiany.

Zarządzanie Kopią zapasową

Kopia zapasowa przechowuje zapasowe kopie plików, które zostały usunięte lub zmodyfikowane podczas leczenia. *Kopia zapasowa* to kopia pliku utworzona przed wyleczeniem lub usunięciem pliku. Kopie zapasowe plików są przechowywane w specjalnym formacie i nie stanowią zagrożenia.

Kopie zapasowe plików są przechowywane w folderze C:\ProgramData\Kaspersky Lab\KES\QB.

Użytkownicy należący do grupy Administratorzy mają nadane pełne uprawnienie dostępu do tego folderu. Ograniczone uprawnienia dostępu do tego folderu są nadawane użytkownikom, których konto zostało użyte do zainstalowania Kaspersky Endpoint Security.

Kaspersky Endpoint Security nie oferuje możliwości skonfigurowania uprawnień dostępu użytkownika do kopii zapasowych plików.


Czasami niemożliwe jest zachowanie integralności plików w trakcie leczenia. W przypadku częściowej lub całkowitej utraty dostępu do istotnych informacji wyleczonego pliku, można spróbować przywrócić plik z jego kopii zapasowej do jego oryginalnego folderu.

Jeśli Kaspersky Endpoint Security działa pod kontrolą Kaspersky Security Center, kopie zapasowe plików mogą być przesyłane do Serwera administracyjnego Kaspersky Security Center. Aby uzyskać więcej informacji na temat zarządzania kopiami zapasowymi plików w Kaspersky Security Center, zapoznaj się z systemem pomocy Kaspersky Security Center.

Konfigurowanie maksymalnego okresu przechowywania plików w Kopii zapasowej

Domyślnie maksymalny czas przechowywania kopii plików w Kopii zapasowej wynosi 30 dni. Po minięciu zdefiniowanego czasu, Kaspersky Endpoint Security usunie najstarsze pliki z Kopii zapasowej.


W celu skonfigurowania maksymalnego okresu przechowywania plików w Kopii zapasowej:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Raporty i pliki danych**.
3. Jeśli chcesz ograniczyć czas przechowywania kopii plików w Kopii zapasowej, w sekcji **Kopia zapasowa** zaznacz pole **Przechowuj obiekty nie dłużej niż N dni**. W polu po prawej stronie pola **Przechowuj obiekty nie dłużej niż N dni** określ maksymalny czas przechowywania kopii plików w Kopii zapasowej.
4. Zapisz swoje zmiany.

Konfigurowanie maksymalnego rozmiaru Kopii zapasowej

Możesz określić maksymalny rozmiar Kopii zapasowej. Domyślnie rozmiar Kopii zapasowej jest nieograniczony. Jeśli maksymalny rozmiar zostanie osiągnięty, Kaspersky Endpoint Security automatycznie usunie najstarsze pliki z Kopii zapasowej, aby maksymalny rozmiar nie został przekroczony.

W celu skonfigurowania maksymalnego rozmiaru Kopii zapasowej:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Raporty i pliki danych**.
3. Jeśli chcesz ograniczyć maksymalny rozmiar Kopii zapasowej, w sekcji **Kopia zapasowa** zaznacz pole **Ogranicz rozmiar Kopii zapasowej do N MB**. Określ maksymalny rozmiar Kopii zapasowej.
4. Zapisz swoje zmiany.

Przywracanie plików z Kopii zapasowej

Jeżeli w pliku zostanie wykryty szkodliwy kod, Kaspersky Endpoint Security zablokuje plik, przypisze do niego stan *Zainfekowany*, umieści jego kopię w folderze Kopii zapasowej i spróbuje go wyleczyć. Po pomyślnym wyleczeniu, stan kopii zapasowej pliku zmieni się na *Wyleczony*. Plik stanie się dostępny w oryginalnym folderze. Jeśli plik nie może zostać wyleczony, Kaspersky Endpoint Security usunie go z jego oryginalnego folderu. Możliwe jest przywrócenie pliku z jego kopii zapasowej do jego oryginalnego folderu.

Pliki ze stanem *Zostanie wyleczony po ponownym uruchomieniu komputera* nie mogą zostać przywrócone. Uruchom ponownie komputer, a stan pliku zmieni się na *Wyleczony* lub *Usunięty*. Możliwe jest także przywrócenie pliku z jego kopii zapasowej do jego oryginalnego folderu.

Po wykryciu szkodliwego kodu w pliku aplikacji ze Sklepu Windows, Kaspersky Endpoint Security natychmiast usunie plik bez przenoszenia jego kopii do Kopii zapasowej. Możesz przywrócić integralność aplikacji ze Sklepu Windows, korzystając z odpowiednich narzędzi systemu operacyjnego Microsoft Windows 8 (zobacz *pliki pomocy dla Microsoft Windows 8*, aby uzyskać szczegółowe informacje dotyczące przywracania aplikacji ze Sklepu Windows).

Zestaw kopii zapasowych plików jest przedstawiony w postaci tabeli. Dla kopii zapasowej pliku wyświetlana jest ścieżka dostępu do oryginalnego folderu pliku. Ścieżka do oryginalnego folderu pliku może zawierać dane osobowe.

Jeśli kilka plików o identycznych nazwach i różnej zawartości zostanie przeniesionych z tego samego folderu do folderu Kopii zapasowej, zostanie przywrócony tylko ten plik, który został ostatnio umieszczony w Kopii zapasowej.

W celu przywrócenia plików z Kopii zapasowej:

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Kopia zapasowa**.
2. To spowoduje otwarcie listy plików w Kopii zapasowej; na tej liście wybierz pliki, które chcesz przywrócić, i kliknij **Przywróć**.

Kaspersky Endpoint Security przywróci wszystkie pliki z wybranych kopii zapasowych do ich oryginalnych folderów.

Usuwanie kopii zapasowych plików z Kopii zapasowej

Kaspersky Endpoint Security automatycznie usuwa kopie zapasowe plików posiadające dowolny stan z Kopii zapasowej po upływie czasu przechowywania, zdefiniowanego w ustawieniach aplikacji. Możesz także ręcznie usunąć dowolną kopię pliku z folderu Kopii zapasowej.

W celu usunięcia kopii zapasowej pliku z Kopii zapasowej:

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Kopia zapasowa**.
2. To spowoduje otwarcie listy plików w Kopii zapasowej; na tej liście wybierz pliki, które chcesz usunąć z Kopii zapasowej, i kliknij **Usuń**. Możesz także usunąć wszystkie pliki z Kopii zapasowej poprzez kliknięcie przycisku **Usuń wszystkie**.

Kaspersky Endpoint Security usunie wybrane kopie zapasowe plików z Kopii zapasowej.

Usługa powiadomień

Podczas działania programu Kaspersky Endpoint Security pojawiają się różnego rodzaju zdarzenia. Powiadomienia o tych zdarzeniach mogą być czysto informacyjne lub zawierać krytyczne informacje. Na przykład, powiadomienia mogą informować o pomyślnej aktualizacji baz danych i modułów aplikacji lub rejestracji błędów komponentów, które muszą być rozwiązane.

Kaspersky Endpoint Security obsługuje rejestrowanie informacji o zdarzeniach w dzienniku aplikacji Microsoft Windows i / lub raporcie zdarzeń Kaspersky Endpoint Security.

Kaspersky Endpoint Security dostarcza powiadomienia w jeden z następujących sposobów:

- Pod postacią komunikatów wyskakujących w obszarze powiadomień paska zadań Microsoft Windows;
- W wiadomości e-mail.


Możliwe jest skonfigurowanie dostarczania powiadomień o zdarzeniach. Metoda dostarczania powiadomień jest skonfigurowana dla każdego typu zdarzenia.

Podczas korzystania z tabeli zdarzeń w celu skonfigurowania usługi powiadamiania można:

- Filtrować zdarzenia według wartości kolumny lub według warunków filtra niestandardowego.
- Użyć funkcji wyszukiwania zdarzeń usługi powiadamiania.
- Sortować zdarzenia usługi powiadamiania.
- Zmienić kolejność i zestaw kolumn wyświetlanych na liście zdarzeń usługi powiadamiania.

Konfigurowanie ustawień dziennika zdarzeń

W celu skonfigurowania ustawień dziennika zdarzeń:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Interfejs**.
3. W sekcji **Powiadomienia** kliknij **Ustawienia powiadomień**.

Moduły i zadania programu Kaspersky Endpoint Security są wyświetlane w lewej części okna. W prawej części okna wyświetlone są zdarzenia wygenerowane dla wybranego komponentu lub zadania.

Zdarzenia mogą zawierać następujące dane użytkownika:

- Ścieżki do plików przeskanowanych przez Kaspersky Endpoint Security.
- Ścieżki do kluczy rejestru zmodyfikowane podczas działania Kaspersky Endpoint Security.
- Nazwę użytkownika Microsoft Windows.
- Adresy stron internetowych otwieranych przez użytkownika.

4. W lewej części okna wybierz komponent lub zadanie, dla którego chcesz skonfigurować ustawienia dziennika zdarzeń.

5. Zaznacz pola obok odpowiednich zdarzeń w kolumnach **Zapisz w raporcie lokalnym** i **Zapisz w dzienniku zdarzeń Windows**.

Zdarzenia, dla których zaznaczono pola w kolumnie **Zapisz w raporcie lokalnym**, są wyświetlane w **Dzienniki aplikacji i usług**, w sekcji **Dziennik zdarzeń aplikacji Kaspersky**. Zdarzenia, dla których zaznaczono pola w kolumnie **Zapisz w dzienniku zdarzeń Windows**, są wyświetlane w **Dzienniki systemu Windows**, w sekcji **Aplikacja**. Aby otworzyć raporty zdarzeń, wybierz **Start** → **Panel sterowania** → **Administracja** → **Podgląd zdarzeń**.

6. Zapisz swoje zmiany.

Konfigurowanie wyświetlania i dostarczania powiadomień

W celu skonfigurowania wyświetlania i dostarczania powiadomień:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Interfejs**.

3. W sekcji **Powiadomienia** kliknij **Ustawienia powiadomień**.

Moduły i zadania programu Kaspersky Endpoint Security są wyświetlane w lewej części okna. W prawej części okna wyświetlone są zdarzenia wygenerowane dla wybranego komponentu lub zadania.

Zdarzenia mogą zawierać następujące dane użytkownika:

- Ścieżki do plików przeskanowanych przez Kaspersky Endpoint Security.
- Ścieżki do kluczy rejestru zmodyfikowane podczas działania Kaspersky Endpoint Security.
- Nazwę użytkownika Microsoft Windows.
- Adresy stron internetowych otwieranych przez użytkownika.

4. W lewej części okna wybierz komponent lub zadanie, dla którego chcesz skonfigurować dostarczanie powiadomień.

5. W kolumnie **Powiadomienie ekranowe** zaznacz pola obok żądanych zdarzeń.

Informacje o wybranych zdarzeniach są wyświetlane w postaci wiadomości wyskakujących w obszarze powiadomień paska zadań Microsoft Windows.

6. W kolumnie **Powiadomienie na e-mail** zaznacz pola obok żądanych zdarzeń.

Informacje o wybranych zdarzeniach są dostarczane za pośrednictwem poczty elektronicznej, jeśli skonfigurowano ustawienia dostarczania powiadomień e-mail.

7. Kliknij **OK**.

8. Jeśli włączyłeś powiadomienia e-mail, skonfiguruj ustawienia dostarczania poczty elektronicznej:


- a. Kliknij przycisk **Ustawienia powiadomiania przy użyciu e-mail**.
- b. Zaznacz pole **Powiadamiaj o zdarzeniach**, aby włączyć dostarczanie informacji o zdarzeniach Kaspersky Endpoint Security wybranych w kolumnie **Powiadomienie na e-mail**.
- c. Określ ustawienia dostarczania powiadomień e-mail.


d. Kliknij **OK**.

9. Zapisz swoje zmiany.

Konfigurowanie wyświetlania komunikatów o stanie aplikacji w obszarze powiadomień

W celu skonfigurowania wyświetlania komunikatów o stanie aplikacji w obszarze powiadomień:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Interfejs**.
3. W sekcji **Pokaż stan aplikacji w obszarze powiadomień** zaznacz pola obok tych kategorii zdarzeń, o których chcesz być informowany w obszarze powiadomień systemu Microsoft Windows.
4. Zapisz swoje zmiany.

Jeśli wystąpią zdarzenia skojarzone z wybraną kategorią, [ikon aplikacji](#) w obszarze powiadomień paska zadań zmieni się na  lub  (w zależności od powagi komunikatu).


Zarządzanie raportami

W raportach zapisywane są informacje o działaniu każdego modułu programu Kaspersky Endpoint Security, zdarzeniach szyfrowania danych, wykonaniu każdego zadania skanowania, zadania aktualizacji oraz zadania sprawdzania integralności, a także o ogólnym działaniu aplikacji.

Raporty są przechowywane w folderze C:\ProgramData\Kaspersky Lab\KES\Report.

Raporty mogą zawierać następujące dane użytkownika:

- Ścieżki do plików przeskanowanych przez Kaspersky Endpoint Security.
- Ścieżki do kluczy rejestru zmodyfikowane podczas działania Kaspersky Endpoint Security.
- Nazwę użytkownika Microsoft Windows.
- Adresy stron internetowych otwieranych przez użytkownika.


Dane w raporcie są przedstawione w formie tabelarycznej. Każdy wiersz tabeli zawiera informacje o oddzielnym zdarzeniu. Atrybuty zdarzenia są zlokalizowane w kolumnach tabeli. Niektóre kolumny zawierają zagnieżdżone kolumny z dodatkowymi atrybutami. Aby wyświetlić dodatkowe atrybuty, należy kliknąć przycisk  znajdujący się obok nazwy kolumny. Zdarzenia zapisywane podczas działania różnych komponentów lub podczas wykonywania różnych zadań posiadają różne zestawy atrybutów.


Dostępne są następujące raporty:

- Raport **Audyt systemu**. Zawiera informacje o zdarzeniach występujących podczas interakcji pomiędzy użytkownikiem i aplikacją oraz o zdarzeniach występujących w trakcie działania aplikacji w ogóle, gdy nie są związane z żadnym konkretnym modułem lub zadaniem Kaspersky Endpoint Security.
- Raporty dotyczące działania komponentów Kaspersky Endpoint Security.
- Raporty zadań Kaspersky Endpoint Security.
- **Raport z szyfrowania danych**. Zawiera informacje o zdarzeniach występujących podczas szyfrowania i deszyfrowania danych.

W raportach używane są następujące priorytety zdarzeń:


 **Zdarzenia informacyjne**. Odpowiednie zdarzenia nie zawierające istotnych informacji.

 **Ostrzeżenia**. Zdarzenia wymagające uwagi użytkownika, ponieważ odzwierciedlają istotną sytuację związaną z działaniem Kaspersky Endpoint Security.

 **Zdarzenia krytyczne**. Zdarzenia posiadające charakter krytyczny i wskazujące na problemy z działaniem Kaspersky Endpoint Security lub luki w ochronie komputera użytkownika.

W celu wygodnego zarządzania raportami możesz zmodyfikować wyświetlanie danych na ekranie w następujące sposoby:

- Filtrować listę zdarzeń według różnych kryteriów.
- Użyć opcji wyszukiwania określonych zdarzeń.
- Przejrzeć wybrane zdarzenie w oddzielnej sekcji.

- Sortować listę zdarzeń według każdej kolumny raportu.
- Wyświetlać i ukrywać zdarzenia grupowane przez filtr zdarzeń przy użyciu przycisku .
- Zmienić kolejność i rozmieszczenie kolumn wyświetlanych w raporcie.

W razie konieczności możesz zapisać wygenerowany raport do pliku. Możesz również [usunąć raport z informacjami](#) z działania komponentów i zadań programu Kaspersky Endpoint Security, które są połączone w grupy.

Jeśli Kaspersky Endpoint Security działa pod zarządzaniem Kaspersky Security Center, informacje o zdarzeniach mogą być przekazywane do Serwera administracyjnego Kaspersky Security Center (więcej informacji znajduje się w [pomocy Kaspersky Security Center](#)^[4]).

Wyświetlanie raportów

Jeśli użytkownik może przeglądać raporty, może także przeglądać wszystkie zdarzenia odzwierciedlone w raportach.

W celu wyświetlenia raportów:

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Raporty**.

2. W lewej części okna **Raporty**, wybierz moduł lub zadanie.

W prawej części okna zostanie wyświetlony raport zawierający listę zdarzeń będących wynikiem działania wybranego komponentu lub wybranego zadania Kaspersky Endpoint Security. Możesz posortować zdarzenia w raporcie w oparciu o wartości w komórkach jednej z kolumn. Domyślnie zdarzenia z raportu są sortowane rosnąco według wartości w komórkach kolumny **Data zdarzenia**.

3. Aby wyświetlić szczegółowe informacje o zdarzeniu, wybierz zdarzenie w raporcie.

W dolnej części okna zostaną wyświetlone informacje podsumowujące zdarzenie.

Konfigurowanie maksymalnego czasu przechowywania raportu

Maksymalny czas przechowywania dla raportów zapisywanych przez Kaspersky Endpoint Security wynosi 30 dni. Po tym czasie Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy z pliku raportu.

W celu zmiany maksymalnego czasu przechowywania raportów:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Raporty i pliki danych**.


3. Jeśli chcesz ograniczyć czas przechowywania raportu, w sekcji **Raporty** zaznacz pole **Przechowuj raporty nie dłużej niż N dni**. Zdefiniuj maksymalny czas przechowywania raportu.

4. Zapisz swoje zmiany.

Konfigurowanie maksymalnego rozmiaru pliku raportu

Możesz określić maksymalny rozmiar pliku zawierającego raport. Domyślnie maksymalny rozmiar pliku raportu wynosi 1024 MB. Aby uniknąć przekroczenia maksymalnego rozmiaru pliku raportu, Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy z pliku raportu po osiągnięciu maksymalnego rozmiaru pliku raportu.

W celu skonfigurowania maksymalnego rozmiaru pliku raportu:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Raporty i pliki danych**.
3. W sekcji **Raporty** zaznacz pole **Ogranicz rozmiar pliku raportu do N MB**, jeśli chcesz ograniczyć rozmiar pliku raportu. Zdefiniuj maksymalny rozmiar pliku raportu.
4. Zapisz swoje zmiany.

Zapisywanie raportu do pliku

Użytkownik jest osobiście odpowiedzialny z zapewnienie bezpieczeństwa informacji z raportu zapisywanego do pliku i częściowo za kontrolowanie i ograniczanie dostępu do tych informacji.

Wygenerowany raport można zapisać do pliku w formacie tekstowym (TXT) lub pliku CSV.

Kaspersky Endpoint Security zapisuje zdarzenia w raporcie w takiej formie, w jakiej są wyświetlane na ekranie: innymi słowy, z takim samym zestawem i sekwencją atrybutów.


W celu zapisania raportu do pliku:

1. W oknie głównym aplikacji, w sekcji **Monitorowanie** kliknij opcję **Raporty**.
2. To spowoduje otwarcie okna; w tym oknie wybierz komponent lub zadanie.
Raport jest wyświetlany w prawej części okna i zawiera listę zdarzeń dotyczących działania wybranego modułu lub zadania Kaspersky Endpoint Security.
3. W razie konieczności możesz zmodyfikować wyświetlanie danych w raporcie poprzez:
 - Filtrowanie zdarzeń
 - Wyszukiwanie zdarzeń
 - Zmienianie kolejności kolumn
 - Sortowanie zdarzeń
4. Kliknij przycisk **Zapisz raport** znajdujący się w prawej górnej części okna.
5. W otwartym oknie określ folder docelowy dla pliku raportu.

6. W polu **Nazwa pliku** wprowadź nazwę pliku raportu.
7. W polu **Typ pliku** wybierz żądany format pliku raportu: TXT lub CSV.
8. Zapisz swoje zmiany.

Czyszczenie raportów

W celu usunięcia informacji z raportów:


1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Raporty i pliki danych**.
3. W sekcji **Raporty** kliknij przycisk **Wyczyść**.
4. Jeśli [Ochrona hasłem jest włączona](#), Kaspersky Endpoint Security może wyświetlić monit o podanie danych uwierzytelniających do konta użytkownika. Aplikacja wyświetla monit o podanie danych uwierzytelniających do konta, jeśli użytkownik nie ma żądanego uprawnienia.

Kaspersky Endpoint Security usunie wszystkie raporty dla wszystkich komponentów i zadań aplikacji.

Autoochrona Kaspersky Endpoint Security

Autoochrona uniemożliwia innym aplikacjom wykonanie działań, które mogą przeszkadzać w działaniu Kaspersky Endpoint Security i, na przykład, usunąć Kaspersky Endpoint Security z komputera. Zestaw dostępnych technologii autoochrony dla Kaspersky Endpoint Security zależy od tego, czy system operacyjny jest 32-bitowy, czy 64-bitowy (patrz tabela poniżej).


Technologie autoochrony Kaspersky Endpoint Security

Technologia	Opis	Komputer z architekturą x86	Komputer z architekturą x64
Mechanizm autoochrony	Technologia blokuje dostęp do następujących komponentów aplikacji: <ul style="list-style-type: none">• pliki w folderze instalacyjnym Kaspersky Endpoint Security i inne pliki aplikacji;• klucze rejestru z wpisami należącymi do aplikacji;• procesy, które aplikacja uruchamia.	✓	✓
AM-PPL (Antimalware Protected Process Light)	Technologia chroni procesy Kaspersky Endpoint Security przed szkodliwymi działaniami. Więcej informacji na temat technologii AM-PPL znajdziesz na stronie internetowej firmy Microsoft  <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">Technologia AM-PPL jest dostępna dla systemu Windows 10 w wersji 1703 (RS2) lub nowszej oraz systemów operacyjnych Windows Server 2019.</div>	✓	✓
Mechanizm ochrony przed zewnętrznym zarządzaniem	Ta technologia chroni uniemożliwia aplikacjom do zdalnego zarządzania (na przykład, TeamViewer lub RemotelyAnywhere) uzyskanie dostępu do Kaspersky Endpoint Security.	✓	– (za wyjątkiem Windows 7)

Włączanie i wyłączanie Autoochrony

Domyślnie Autoochrona programu Kaspersky Endpoint Security jest włączona.

W celu włączenia lub wyłączenia Autoochrony:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ogólne**.
3. Użyj pola **Włącz autoochronę**, aby włączyć lub wyłączyć mechanizm autoochrony.
4. Zapisz swoje zmiany.

Włączanie i wyłączanie obsługi AM-PPL

Kaspersky Endpoint Security obsługuje technologię Antimalware Protected Process Light (zwana dalej „AM-PPL”) firmy Microsoft. AM-PPL chroni procesy Kaspersky Endpoint Security przed szkodliwymi działaniami (na przykład, zakończeniem działania aplikacji). AM-PPL pozwala na uruchamianie tylko zaufanych procesów. Procesy Kaspersky Endpoint Security są podpisywane zgodnie z wymaganiami dotyczącymi zabezpieczeń systemu Windows, dlatego są zaufane. Więcej informacji na temat technologii AM-PPL znajdziesz na [stronie internetowej firmy Microsoft](#). Domyślnie technologia AM-PPL jest włączona.

Kaspersky Endpoint Security ma również wbudowane mechanizmy ochrony procesów aplikacji. Obsługa AM-PPL pozwala delegować funkcje ochrony procesów do systemu operacyjnego. W ten sposób można zwiększyć szybkość aplikacji i zmniejszyć zużycie zasobów komputerowych.

Technologia AM-PPL jest dostępna dla systemu Windows 10 w wersji 1703 (RS2) lub nowszej oraz systemów operacyjnych Windows Server 2019.

W celu włączenia lub wyłączenia technologii AM-PPL:

1. [Wyłącz mechanizm autoochrony aplikacji.](#)

Mechanizm autoochrony zapobiega modyfikowaniu i usuwaniu procesów aplikacji w pamięci komputera, w tym zmianie stanu AM-PPL.

2. Uruchom wiersz poleceń (cmd.exe) jako administrator.

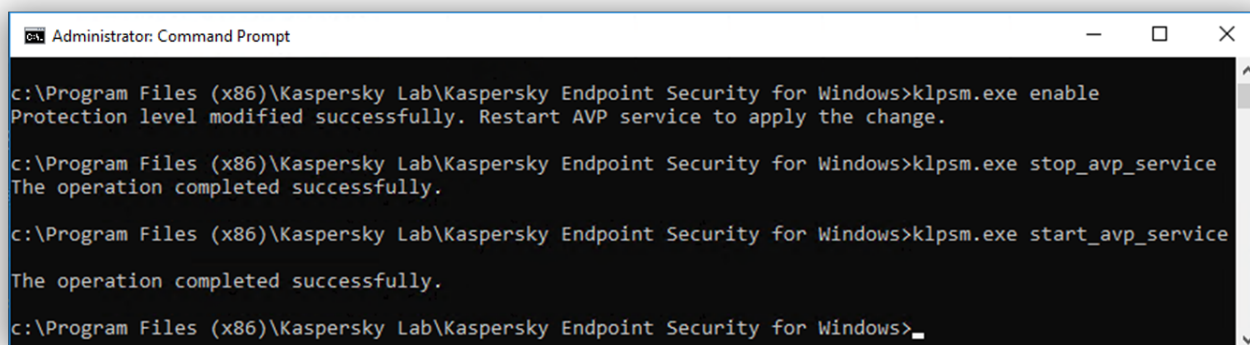
3. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.

4. W wierszu poleceń wpisz następujące polecenie:

- `klpsm.exe enable` - włącza obsługę technologii AM-PPL (patrz rysunek poniżej).
- `klpsm.exe disable` - wyłącza obsługę technologii AM-PPL.

5. Uruchom ponownie Kaspersky Endpoint Security.

6. [Wznów mechanizm autoochrony aplikacji.](#)



```
Administrator: Command Prompt
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe enable
Protection level modified successfully. Restart AVP service to apply the change.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe stop_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>klpsm.exe start_avp_service
The operation completed successfully.
c:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>
```

Włączanie obsługi technologii AM-PPL


Włączanie i wyłączanie ochrony przed zewnętrznym zarządzaniem

Ochrona przed zewnętrznym zarządzaniem uniemożliwia aplikacjom do zdalnego zarządzania (na przykład, TeamViewer lub RemotelyAnywhere) uzyskanie dostępu do Kaspersky Endpoint Security. Ta technologia zawiera następujące funkcje ochrony przed zewnętrznym zarządzaniem:

- Ochrona przed modyfikacją ustawień Kaspersky Endpoint Security.
- Ochrona usług Kaspersky Endpoint Security (takich jak usługa avp).
- Ochrona procesów aplikacji.

Ochrona przed zewnętrznym zarządzaniem jest dostępna tylko dla komputerów działających pod kontrolą 32-bitowych systemów operacyjnych, za wyjątkiem Windows 7. Jeśli chodzi o system Windows 7, to technologia jest dostępna dla wersji 32-bitowej i 64-bitowej.

W celu włączenia lub wyłączenia ochrony przed zdalnym zarządzaniem:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ogólne**.
3. Użyj pola **Zezwól na zarządzanie ustawieniami Kaspersky Endpoint Security za pomocą aplikacji do zdalnego zarządzania**, aby włączyć lub wyłączyć ochronę przed zewnętrznym zarządzaniem.

Jeśli pole jest zaznaczone, możesz użyć aplikacji do zdalnego zarządzania w celu skonfigurowania programu Kaspersky Endpoint Security i zarządzania jego usługami i procesami.

Jeśli pole jest odznaczone, ochrona przed zewnętrznym zarządzaniem uniemożliwia aplikacjom do zdalnej administracji uzyskanie dostępu do Kaspersky Endpoint Security. Możesz zezwolić na konfigurowanie Kaspersky Endpoint Security przy użyciu określonych aplikacji do zdalnej administracji. W tym celu musisz [dodać aplikację do zdalnej administracji do listy zaufanych](#). W tym przypadku ochrona przed zdalną administracją będzie dalej uniemożliwiać aplikacjom do zdalnej administracji uzyskanie dostępu do usług i procesów Kaspersky Endpoint Security.

4. Użyj pola **Włącz możliwość zewnętrznej kontroli usługi**, aby włączyć lub wyłączyć ochronę usług Kaspersky Endpoint Security przed zewnętrznym zarządzaniem.

Aby zakończyć działanie aplikacji z poziomu wiersza poleceń, wyłącz ochronę usług Kaspersky Endpoint Security przed zewnętrznym zarządzaniem.


5. Zapisz swoje zmiany.

W wyniku tego działania, jeśli włączona jest ochrona przed zdalnym zarządzaniem, Kaspersky Endpoint Security uniemożliwia wskaźnikowi myszy najechanie na okno aplikacji. Jeśli zdalny użytkownik podejmie próbę zakończenia działania usługi aplikacji, zostanie wyświetlone okno systemowe z komunikatem o błędzie.



Obsługiwanie aplikacji do zdalnej administracji

Czasami możesz potrzebować aplikacji do zdalnej administracji, gdy włączona jest ochrona przed zewnętrznym zarządzaniem.

W celu włączenia działania aplikacji do zdalnej administracji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Zagrożenia i wykluczenia**.
3. W sekcji **Wykluczenia** kliknij odnośnik **Określ zaufane aplikacje**.
4. W oknie kliknij przycisk **Dodaj**.

5. Wybierz plik wykonywalny aplikacji do zdalnej administracji.

Możesz również ręcznie wprowadzić ścieżkę. Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki  i .

6. Zaznacz pole **Nie monitoruj aktywności aplikacji**.

7. Zapisz swoje zmiany.

Działanie Kaspersky Endpoint Security i kompatybilność z innymi aplikacjami

Wydajność programu Kaspersky Endpoint Security

Wydajność Kaspersky Endpoint Security wiąże się z liczbą typów wykrywanych szkodliwych obiektów, zużyciem energii i wykorzystaniem zasobów komputera.

Wybieranie typów wykrywanych obiektów

Kaspersky Endpoint Security umożliwia dostosowanie ochrony komputera i wybranie [typów obiektów](#) wykrywanych przez aplikację podczas działania. Kaspersky Endpoint Security zawsze skanuje system operacyjny w poszukiwaniu wirusów, robaków i trojanów. Nie możesz wyłączyć skanowania tych typów obiektów. Takie szkodliwe oprogramowanie może wyrządzić znaczne szkody w komputerze. Aby zwiększyć ochronę komputera, możesz poszerzyć zakres wykrywanych typów obiektów, włączając monitorowanie legalnych aplikacji, które cyberprzestępca może przejąć w celu wyrządzenia szkód lub kradzieży danych.

Korzystanie z trybu oszczędzania energii

Zużycie energii przez aplikację jest kluczowe dla komputerów przenośnych. Zaplanowane zadania z Kaspersky Endpoint Security zazwyczaj wykorzystują dużą ilość zasobów. Aby oszczędzać energię w trakcie pracy na baterii, możesz użyć trybu oszczędzania energii.

W trybie oszczędzania energii automatycznie odraczane są następujące zadania:

- Zadanie aktualizacji;
- Zadanie Pełne skanowanie;
- Zadanie Skanowanie obszarów krytycznych;
- Zadanie Skanowanie obiektów;
- Zadanie Sprawdzanie integralności.

Niezależnie od tego, czy tryb oszczędzania energii jest włączony, Kaspersky Endpoint Security wstrzymuje zadania szyfrowania po przejściu komputera przenośnego do trybu pracy na bateriach. Aplikacja wznowia zadania szyfrowania po przejściu komputera przenośnego z trybu pracy na bateriach do trybu głównego.

Udostępnianie zasobów komputera innym aplikacjom

Wykorzystanie zasobów komputera przez Kaspersky Endpoint Security może wpłynąć na działanie innych aplikacji. Aby rozwiązać problem równoczesnego wykonywania działań w trakcie dużego obciążenia procesora i podsystemów dysku, Kaspersky Endpoint Security może wstrzymać zaplanowane zadania i udostępnić zasoby innym aplikacjom.

Jednak istnieją takie aplikacje, które uruchamiają się natychmiast po zwolnieniu się zasobów procesora i działają w tle. Aby zapobiec uruchamianiu skanowania w zależności od działania innych aplikacji, lepiej nie udostępniać zasobów systemu operacyjnego takim aplikacjom.

W razie konieczności możesz uruchomić zadania ręcznie.

Używanie zaawansowanej technologii leczenia

Obecnie szkodliwe aplikacje mogą wnikać do najniższych poziomów systemu operacyjnego, co praktycznie uniemożliwia jego usunięcie. Po wykryciu szkodliwej aktywności w systemie operacyjnym, Kaspersky Endpoint Security wykonuje zaawansowaną procedurę leczenia, która korzysta ze specjalnej technologii zaawansowanego leczenia. *Technologia zaawansowanego leczenia* służy do usuwania z systemu operacyjnego szkodliwych aplikacji, które już uruchomiły swoje procesy w pamięci RAM i nie pozwalają aplikacji Kaspersky Endpoint Security na usunięcie ich przy pomocy innych metod. W rezultacie zagrożenie zostanie zneutralizowane. W trakcie działania Zaawansowanego leczenia zaleca się nie uruchamiać nowych procesów ani nie modyfikować rejestru systemu operacyjnego. Technologia zaawansowanego leczenia wykorzystuje dużą ilość zasobów systemu operacyjnego, co może spowolnić inne aplikacje.



Po zakończeniu procesu Zaawansowanego leczenia na komputerze działającym pod kontrolą Microsoft Windows dla stacji roboczych, Kaspersky Endpoint Security poprosi użytkownika o pozwolenie na ponowne uruchomienie komputera. Po ponownym uruchomieniu systemu Kaspersky Endpoint Security wykryje pliki szkodliwego oprogramowania i rozpocznie "lekkie" pełne skanowanie komputera.

Ponowne uruchomienie nie jest możliwe na komputerze działającym pod kontrolą Microsoft Windows dla serwerów z powodu specyfiki Kaspersky Endpoint Security. Nieplanowane ponowne uruchomienie serwera plików może doprowadzić do tymczasowej niedostępności danych serwera plików lub utraty niezapisanych danych. Zaleca się uruchamiać serwer plików trzymając się ściśle ustalonego terminarza. Z tego powodu technologia zaawansowanego leczenia jest domyślnie wyłączona dla serwerów plików.

Jeśli aktywna infekcja zostanie wykryta na serwerze plików, zdarzenie zostanie przesłane do Kaspersky Security Center wraz z informacją, że konieczne jest Zaawansowane leczenie. Aby wyleczyć aktywną infekcję na serwerze, włącz technologię zaawansowanego leczenia dla serwerów i uruchom grupowe zadanie *Skanowania antywirusowego* w momencie wygodnym dla użytkowników serwera.

Wybieranie typów wykrywanych obiektów

W celu wybrania typów wykrywanych obiektów:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Zagrożenia i wykluczenia**.
3. W sekcji **Rodzaje wykrywanych obiektów** zaznacz pola obok typów obiektów, które Kaspersky Endpoint Security ma wykrywać:
 - [Wirusy i robaki](#) 

Podkategoria: wirusy i robaki (wirusy_i_robaki)

Poziom zagrożenia: wysoki

Klasyczne wirusy i robaki wykonują akcje nieautoryzowane przez użytkownika. Mogą one tworzyć swoje kopie, które także są zdolne do powielania się.

Klasyczny wirus

Po przeniknięciu klasycznego wirusa do komputera, infekuje on plik, aktywuje się w nim, wykonuje szkodliwe działania i dodaje swoje kopie do innych plików.

Klasyczny wirus rozprzestrzenia się jedynie na zasobach lokalnych komputera; nie może sam przedostać się na inne komputery. Przedostanie się takiego wirusa na inny komputer jest możliwe, jeśli doda on swoją kopię do pliku przechowywanego w folderze współdzielonym lub na nośniku CD, albo gdy użytkownik wyśle wiadomość z zainfekowanym załącznikiem.

Kod klasycznego wirusa może przedostać się do różnych obszarów komputerów, systemów operacyjnych lub aplikacji. W zależności od środowiska wirusy dzieli się na *wirusy plikowe*, *wirusy sektora startowego*, *wirusy skryptowe* oraz *makrowirusy*.

Wirusy mogą infekować pliki, korzystając z szerokiej gamy technik. *Wirusy nadpisujące* zapisują swój kod na kodzie zainfekowanego pliku, wymazując jego zawartość. Zainfekowany plik przestaje poprawnie działać oraz nie ma możliwości jego przywrócenia. *Wirusy pasożyty* modyfikują pliki, zezwalając na ich pełne lub częściowe działanie. *Wirusy towarzysze* nie modyfikują plików, lecz tworzą ich kopie. Kiedy otwarty zostanie zainfekowany plik, uruchomiona zostanie jego kopia (czyli wirus). Można wyróżnić również następujące typy wirusów: *wirusy-odsyłacze*, *wirusy plików OBJ*, *wirusy bibliotek LIB*, *wirusy infekujące kody źródłowe* oraz wiele innych.

Robak

Podobnie jak w przypadku klasycznego wirusa, kod robaka zostaje aktywowany i wykonuje on szkodliwe działania po przeniknięciu do komputera. Robaki noszą taką nazwę z powodu swojej zdolności do "przepełzania" z jednego komputera na inny i rozprzestrzeniania swoich kopii za pośrednictwem wielu kanałów danych bez wiedzy użytkownika.

Główną cechą, która umożliwia rozróżnianie typów robaków, jest ich sposób rozprzestrzeniania się. Następująca tabela zawiera przegląd różnych typów robaków, klasyfikowanych zgodnie ze sposobem rozprzestrzeniania się.

Sposoby rozprzestrzeniania się robaka

Typ	Nazwa	Opis
Email-Worm	Email-Worm	Rozprzestrzeniają się poprzez pocztę elektroniczną. Zainfekowana wiadomość zawiera załączony plik z kopią robaka lub odnośnik do pliku znajdującego się na stronie internetowej, która może być albo przechwycona przez hakerów, albo stworzona specjalnie w tym celu. Jeśli otworzysz zainfekowany plik, robak zostanie aktywowany. Po kliknięciu odsyłacza, pobraniu i otwarciu pliku, robak również rozpoczyna swoją szkodliwą działalność. Następnie zaczyna rozprzestrzeniać swoje kopie, wyszukując kolejne adresy e-mail i wysyłając na nie zainfekowane wiadomości.
IM-Worm	Robaki klientów komunikatorów internetowych	Rozprzestrzeniają się poprzez klienty komunikatorów internetowych.

		Z reguły robaki te za pośrednictwem listy kontaktów użytkownika wysyłają wiadomości zawierające odnośnik do pliku ze swoją kopią. Po pobraniu i otwarciu takiego pliku przez użytkownika, robak jest aktywowany.
IRC-Worm	Robaki czatu internetowego	Rozprzestrzeniają się za pośrednictwem kanału IRC (Internet Relay Chats) – czyli usługi sieciowej pozwalającej na komunikowanie się w internecie w czasie rzeczywistym. Robaki te publikują w czacie internetowym pliki zawierające ich kopie lub odnośniki do pliku. Po pobraniu i otwarciu takiego pliku przez użytkownika, robak jest aktywowany.
Net-Worm	Robaki sieciowe	Rozprzestrzeniają się one w sieciach komputerowych. W przeciwieństwie do innych rodzajów robaków, typowy robak sieciowy rozprzestrzenia się bez udziału użytkownika. Skanuje on sieć lokalną w poszukiwaniu komputerów z programami zawierającymi luki. W tym celu wysyła on specjalny pakiet sieciowy (exploit) zawierający kod robaka lub część kodu. Jeśli komputer posiadający luki znajduje się w sieci, otrzyma taki pakiet sieciowy. Po przeprowadzeniu pełnej penetracji komputera, jest on aktywowany.
P2P-Worm	Robaki sieci wymiany plików	Rozprzestrzeniają się one w sieciach peer-to-peer. Aby dostać się do sieci P2P, robak kopiuje się do foldera wymiany plików, który zazwyczaj znajduje się na komputerze użytkownika. Sieć P2P wyświetli informacje o tym pliku, aby użytkownik "znalazł" zainfekowany plik w sieci, pobrał go i otworzył. Bardziej zaawansowane robaki emulują protokół sieciowy konkretnej sieci P2P: wyświetlają pozytywne wyniki wyszukiwanego obiektu i proponują pobranie swoich własnych kopii.
Robak	Inne rodzaje robaków	Inne rodzaje robaków obejmują: <ul style="list-style-type: none"> • Robaki rozprzestrzeniające swoje kopie w zasobach sieciowych. Przy użyciu funkcji systemu operacyjnego skanują dostępne foldery sieciowe, łączą się z komputerami w Internecie i próbują uzyskać pełen dostęp do ich dysków. W przeciwieństwie do opisanych wyżej robaków, inne typy robaków nie aktywują się automatycznie, lecz w momencie, gdy użytkownik otworzy plik zawierający kopię robaka. • Robaki, które nie rozprzestrzeniają się w żaden z powyższych sposobów (na przykład te robaki, które rozprzestrzeniają się poprzez telefony komórkowe).

- [Trojany](#) 

Podkategoria: Trojany

Poziom zagrożenia: wysoki

W przeciwieństwie do wirusów i robaków, trojany nie tworzą swoich kopii. Przenikają one do komputera, na przykład, za pośrednictwem wiadomości e-mail lub przeglądarki internetowej po otwarciu zainfekowanej strony. Trojany uruchamiają się przy udziale użytkownika. Zaczynają wykonywać szkodliwe działania zaraz po uruchomieniu.

Różne programy typu trojan zachowują się odmiennie na zainfekowanych komputerach. Głównym zadaniem trojanów jest blokowanie, modyfikowanie lub niszczenie informacji, wyłączanie komputera lub sieci. Poza tym, trojany otrzymują lub wysyłają pliki, uruchamiają je, wyświetlają wiadomości na ekranie, pobierają i instalują aplikacje, uruchamiają ponownie komputer oraz żądają połączenia ze stroną internetową.

Hakerzy często używają "zestawów" trojanów.

Typowe zachowanie trojanów opisane jest w poniższej tabeli.

Typy zachowań trojanów na zainfekowanym komputerze

Typ	Nazwa	Opis
Trojan-ArcBomb	Trojany – "archiwa-bomby"	Archiwa, które po rozpakowaniu zwiększają swój rozmiar, co zakłóca działanie komputera. Podczas próby rozpakowania takiego archiwum komputer może spowolnić swoje działanie lub całkowicie się zawiesić, a dysk twardy może zostać wypełniony "pustymi" danymi. Archiwa-bomby są szczególnie niebezpieczne dla serwerów poczty i plików. Jeśli serwer korzysta z automatycznego systemu przetwarzania informacji przychodzących, archiwum-bomba może zatrzymać jego działanie.
Backdoor	Trojany do zdalnej administracji	Uważa się, że jest to najbardziej niebezpieczny rodzaj trojanów. Dzięki swoim funkcjom są one podobne do programów służących do zdalnej administracji aplikacji zainstalowanych na komputerach. Trojany instalują się na komputerze bez wiedzy użytkownika i pozwalają hakerowi na jego zdalne zarządzanie.
Trojan	Trojany	Do trojanów zaliczają się następujące szkodliwe aplikacje: <ul style="list-style-type: none">• Klasyczne trojany. Wykonują tylko podstawowe funkcje charakterystyczne dla trojanów: blokują, modyfikują lub niszczą informacje, wyłączają komputery lub sieci. W odróżnieniu od trojanów opisanych w tabeli, nie charakteryzują się żadnymi zaawansowanymi funkcjami.• Wszechstronne trojany. Posiadają zaawansowane funkcje typowe dla kilku rodzajów trojanów.
Trojan-Ransom	Trojany przeznaczone do wyłudzenia pieniędzy	Jako "zakładników" biorą one informacje użytkownika, modyfikują lub blokują je, albo tak wpływają na działanie komputera, że użytkownik nie może korzystać z informacji. Cyberprzestępca żąda okupu od użytkownika, obiecując, że wyśle aplikację, która przywróci działanie komputera oraz przechowywane na nim dane.
Trojan-Clicker	Trojany klikające	Łączą się one ze stronami internetowymi albo przez wysłanie polecenia do przeglądarki albo przez zmianę adresów stron

		znajdujących się w plikach systemowych. Przy użyciu tych programów hakerzy przeprowadzają ataki sieciowe i zwiększają ranking stron internetowych celem zwiększenia liczby wyświetlania banerów reklamowych.
Trojan-Downloader	Trojany pobierające	Uzyskują dostęp do strony internetowej cyberprzestępcy, pobierają z niej szkodliwe aplikacje i instalują je na komputerze użytkownika. Mogą zawierać nazwę pliku szkodliwej aplikacji do pobrania lub uzyskać ją z otwartej strony internetowej.
Trojan-Dropper	Trojany droppery	Zawierają inne trojany, które instalują na dysku twardym. Hakerzy mogą użyć tego typu trojanów do następujących celów: <ul style="list-style-type: none"> • Zainstalowania szkodliwej aplikacji bez wiedzy użytkownika: Trojan-Dropper to typ programów, które nie wyświetlają żadnych wiadomości lub wyświetlają fałszywe komunikaty informujące, na przykład, o błędzie w archiwum lub niekompatybilnej wersji systemu operacyjnego. • Ochrony innych znanych szkodliwych aplikacji przed wykryciem przez ochronę komputera: nie wszystkie programy antywirusowe są w stanie wykryć szkodliwą aplikację wewnątrz aplikacji Trojan-Dropper.
Trojan-Notifier	Trojany powiadamiające	Informują hakera o możliwości dostępu do zainfekowanego komputera, wysyłając do niego informacje o tym komputerze: adres IP, numer otwartego portu lub adres e-mail. Komunikują się z hakerem, na przykład, za pośrednictwem wiadomości e-mail, serwera FTP lub jego strony internetowej. Trojany typu Notifier często są wykorzystywane w zestawach złożonych z kilku trojanów. Powiadamiają one hakera, że inne trojany zostały pomyślnie zainstalowane na komputerze użytkownika.
Trojan-Proxy	Trojany proxy	Umożliwiają one hakerowi uzyskanie anonimowego dostępu do stron internetowych przy użyciu komputera użytkownika i są często używane do wysyłania spamu.
Trojan-PSW	Oprogramowanie kradnące hasła	Oprogramowanie kradnące hasła to rodzaj trojanów kradnących konta użytkownika, na przykład dane rejestracyjne oprogramowania. Takie trojany odnajdują w plikach systemowych i rejestrują poufne dane, a następnie wysyłają je do atakującego, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej. Niektóre z tych trojanów podzielone są na kategorie oddzielnych typów opisanych w tej tabeli. Należą do nich Trojany kradnące konta bankowe (Trojan-Banker), trojany kradnące informacje od użytkowników komunikatorów internetowych (Trojan-IM) oraz trojany kradnące informacje od graczy online (Trojan-GameThief).
Trojan-Spy	Trojany szpiegujące	Szpiegują one użytkownika, zbierając informacje o jego działaniach podczas pracy na komputerze. Mogą przechwytywać dane wprowadzane przez użytkownika przy użyciu klawiatury, tworzyć zrzuty ekranu lub tworzyć listę aktywnych aplikacji. Po zebraniu informacji, wysyłają je do hakera, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.

Trojan-DDoS	Ataki sieciowe	<p>Wysyłają one liczne żądania z komputera użytkownika na serwer zdalny. Serwer nie ma wystarczającej ilości zasobów do przetworzenia wszystkich żądań, w rezultacie przestaje działać (Denial-of-Service lub DoS). Hakerzy często infekują wiele komputerów dzięki takim programom, przez co mogą wykorzystać te komputery do jednoczesnego ataku na pojedynczy serwer.</p> <p>Programy DoS przeprowadzają atak z jednego komputera za wiedzą użytkownika. Programy DDoS (Distributed DoS) przeprowadzają rozproszone ataki z różnych komputerów bez wiedzy użytkownika zainfekowanego komputera.</p>
Trojan-IM	Trojany kradnące informacje od użytkowników komunikatorów internetowych	Kradną numery kont i hasła użytkowników klientów komunikatorów internetowych. Przesyłają dane hakerowi, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Rootkit	Rootkity	Ukrywają inne szkodliwe aplikacje i ich aktywność, przedłużając ich obecność w systemie. Mogą również ukrywać pliki i procesy w pamięci zainfekowanego komputera lub kluczach rejestru. Rootkity mogą ukrywać wymianę danych pomiędzy aplikacjami znajdującymi się na komputerze użytkownika i innymi komputerami podłączonymi do sieci.
Trojan-SMS	Trojany wysyłające wiadomości SMS	Infekują one telefony komórkowe, wysyłając wiadomości SMS na numery o podwyższonej opłacie.
Trojan-GameThief	Trojany kradnące informacje od osób grających w sieci	Kradną dane uwierzytelniające kont osób grających w sieci, po czym wysyłają je hakerowi za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Trojan-Banker	Trojany kradnące konta bankowe	Kradną dane konta bankowego lub dane systemu płatności elektronicznych, po czym wysyłają je cyberprzestępcy za pośrednictwem poczty elektronicznej, serwera FTP, jego strony internetowej lub przy użyciu innych metod.
Trojan-Mailfinder	Trojany zbierające adresy e-mail	Zbierają one adresy e-mail przechowywane na komputerze i wysyłają je hakerowi, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej. Na zebrane adresy hakerzy mogą wysyłać spam.

- [Szkodliwe narzędzia](#) 

Podkategoria: Szkodliwe narzędzia

Poziom zagrożenia: średni

W odróżnieniu od innych typów szkodliwego oprogramowania, szkodliwe narzędzia nie wykonują swoich akcji zaraz po uruchomieniu. Mogą być bezpiecznie przechowywane i uruchamiane na komputerze użytkownika. Hakerzy często używają funkcji tych programów do tworzenia wirusów, robaków i trojanów oraz do przeprowadzania ataków sieciowych na serwery zdalne, łamania zabezpieczeń komputerów lub wykonywania innych szkodliwych działań.

Różne funkcje szkodliwych narzędzi pogrupowane są według typów opisanych w poniższej tabeli.

Funkcje szkodliwych narzędzi

Typ	Nazwa	Opis
Konstruktor	Konstruktory	Umożliwiają utworzenie nowych wirusów, robaków i trojanów. Niektóre konstruktory posiadają standardowy interfejs oparty na oknach, w którym użytkownik może wybrać typ szkodliwej aplikacji, jaki chce stworzyć, sposób przeciwdziałania debuggerom oraz inne funkcje.
Dos	Ataki sieciowe	Wysyłają one liczne żądania z komputera użytkownika na serwer zdalny. Serwer nie ma wystarczającej ilości zasobów do przetworzenia wszystkich żądań, w rezultacie przestaje działać (Denial-of-Service lub DoS).
Exploit	Exploity	<p>Exploit jest zestawem danych lub kodem programu używającym luki aplikacji, w której jest przetwarzany, do wykonania szkodliwych działań na komputerze. Na przykład, exploit może odczytywać lub zapisywać pliki lub uzyskiwać dostęp do "zainfekowanych" stron internetowych.</p> <p>Różne exploity używają luk w różnych aplikacjach lub usługach sieciowych. Wyglądający jak pakiet sieciowy exploit wysyłany jest przez sieć w poszukiwaniu takich komputerów, których usługi sieciowe posiadają luki. Exploit w pliku DOC używa luk występujących w edytorach tekstu. Po otwarciu przez użytkownika zainfekowanego pliku, może on zacząć wykonywać zaprogramowane przez hakera działania. Exploit osadzony w wiadomości elektronicznej wyszukuje luki w dowolnym kliencie pocztowym. Po otwarciu przez użytkownika zainfekowanego pliku w tym programie pocztowym, wykonuje on szkodliwe działanie.</p> <p>Robaki Net-Worms rozprzestrzeniają się w sieci przy pomocy exploitów. <i>Exploity</i> Nuker są pakietami sieciowymi wyłączającymi komputery.</p>
FileCryptor	Narzędzia szyfrujące	Szyfrują one inne szkodliwe aplikacje, aby ukryć je przed programem antywirusowym.
Flooder	Programy "zaśmiecające" sieci	<p>Wysyłają one wiele wiadomości przez kanały sieciowe. Do tego typu narzędzi należy, na przykład, program zaśmiecający Internet Relay Chats (IRC).</p> <p>Wśród narzędzi typu Flooder nie ma programów "zaśmiecających" kanały używane przez programy pocztowe, komunikatory internetowe i systemy komunikacji mobilnej. Programy te wyróżnione są jako oddzielne typy opisane w tej tabeli (Email-Flooder, IM-Flooder oraz SMS-Flooder).</p>

HackTool	Narzędzia hakerskie	Pozwalają na złamanie zabezpieczeń komputera, na którym są zainstalowane, lub na zaatakowanie innego komputera (na przykład, dodając nowe konta systemowe bez wiedzy użytkownika lub wymazując logi systemowe, aby ukryć ślady obecności w systemie operacyjnym). Ten typ narzędzi zawiera sniffery posiadające szkodliwe funkcje, jak choćby przechwytywanie haseł. Sniffery to programy umożliwiające przeglądanie ruchu sieciowego.
Hoax	Żarty (Hoaxes)	Alarmują użytkownika przy użyciu wiadomości podobnej do tej, która używana jest w przypadku wykrycia wirusa: mogą "wykryć wirusa" w nienaruszonym pliku lub powiadomić o formatowaniu dysku, które w rzeczywistości nie ma miejsca.
Spoofier	Narzędzia służące do spoofingu	Wysyłają wiadomości i żądania sieciowe z fałszywym adresem nadawcy. Hakerzy używają narzędzi do spoofingu, na przykład, aby móc podać się za prawdziwych nadawców wiadomości.
VirTool	Narzędzia do modyfikowania szkodliwych aplikacji	Umożliwiają modyfikowanie innego szkodliwego oprogramowania w celu ukrycia go przed aplikacjami antywirusowymi.
Email-Flooder	Programy "zaśmiecające" adresy e-mail	"Zaśmiecają" różne adresy e-mail poprzez wysyłanie na nie licznych wiadomości. Duża liczba wiadomości przychodzących uniemożliwia przejrzanie użytecznych wiadomości znajdujących się w skrzynce odbiorczej.
IM-Flooder	Programy "zaśmiecające" ruch wiadomościami klientów komunikatorów internetowych	Wysyłają niechciane wiadomości do użytkowników klientów komunikatorów. Duża liczba odbieranych wiadomości uniemożliwia przeczytanie użytecznych wiadomości.
SMS-Flooder	Programy "zaśmiecające" ruch wiadomościami SMS	Wysyłają one liczne wiadomości SMS na telefony komórkowe.

- [Adware](#) 

Podkategoria: oprogramowanie reklamujące (Adware);

Poziom zagrożenia: średni

Oprogramowanie Adware wyświetla informacje reklamowe użytkownikowi. Programy adware wyświetlają banery reklamowe w interfejsach innych programów i przekierowują wyszukiwanie na strony reklamowe. Niektóre z nich zbierają informacje marketingowe o użytkowniku i wysyłają je do programisty. Do gromadzonych informacji mogą należeć: nazwy stron odwiedzanych przez użytkownika lub wyszukiwana przez niego treść. W odróżnieniu od programów typu Trojan-Spy, programy adware przesyłają te informacje do twórcy za zgodą użytkownika.

- [Auto-dialery](#) 

Podkategoria: legalne oprogramowanie, które może zostać wykorzystane przez cyberprzestępców do uszkodzenia komputera i prywatnych danych.

Poziom zagrożenia: średni

Wiele z tych programów to nieszkodliwe oprogramowanie, z którego korzysta wielu użytkowników. Do tych programów zaliczają się: klienci IRC, auto-dialery, programy pobierające pliki, monitory aktywności systemu komputerowego, narzędzia do haseł, serwery usług FTP, HTTP i Telnet.

Jednakże, jeśli haker uzyska dostęp do tego typu programów lub jeśli zainstaluje te programy na komputerze użytkownika, to niektóre z ich funkcji mogą zostać użyte do naruszenia ochrony.

Aplikacje te mają różne funkcje; ich typy zostały opisane w poniższej tabeli.

Typ	Nazwa	Opis
Client-IRC	Klienci czatów internetowych	Użytkownicy instalują programy tego typu, aby móc rozmawiać z innymi w czasie rzeczywistym. Hakerzy używają ich do rozsyłania szkodliwych programów.
Dialer	Auto-dialery	Mogą nawiązywać połączenie telefoniczne za pośrednictwem modemu w trybie ukrycia.
Downloader	Programy do pobierania	Mogą pobierać pliki ze stron internetowych w trybie ukrycia.
Monitor	Programy do monitorowania	Umożliwiają monitorowanie aktywności na komputerze, na którym są zainstalowane (sprawdzają, które aplikacje są aktywne i w jaki sposób wymieniają dane z aplikacjami zainstalowanymi na innych komputerach).
PSWTool	Programy do przywracania haseł	Umożliwiają przeglądanie i przywracanie zapomnianych haseł. Hakerzy umieszczają je na komputerze w tym samym celu, w sposób niezauważalny dla użytkownika.
RemoteAdmin	Programy do zdalnej administracji	Są używane przez administratorów systemów. Programy te pozwalają uzyskać dostęp do interfejsu zdalnego komputera w celu jego monitorowania i zarządzania. W tym właśnie celu hakerzy niezauważenie umieszczają je na komputerze użytkownika. Legalne programy do zdalnej administracji różnią się od trojanów typu backdoor do zdalnej administracji. Trojanzy potrafią niezależnie spenetrować system i zainstalować się; legalne programy nie potrafią tego.
Server-FTP	Serwery FTP	Działają jak serwery FTP. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu FTP.
Server-Proxy	Serwery proxy	Działają jak serwery proxy. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
Server-Telnet	Serwery Telnet	Działają jak serwery Telnet. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu Telnet.
Server-Web	Serwery sieciowe	Działają jak serwery sieciowe. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu HTTP.
RiskTool	Narzędzia	Umożliwiają one użytkownikowi korzystanie z dodatkowych

	wykorzystywane do pracy na lokalnym komputerze	funkcji podczas jego pracy na komputerze. Narzędzia te pozwalają użytkownikowi ukryć pliki lub okna uruchomionych aplikacji i zakończyć aktywne procesy.
NetTool	Narzędzia sieciowe	Umożliwiają użytkownikowi korzystanie z dodatkowych funkcji podczas pracy z innymi komputerami w sieci. Posiadają one także możliwość ich ponownego uruchomienia, wykrywania otwartych portów oraz uruchamiania aplikacji zainstalowanych na komputerach.
Client-P2P	Klienci sieciowe P2P	Pozwalają pracować w sieciach peer-to-peer. Mogą być wykorzystywane przez hakerów do rozprzestrzeniania szkodliwego oprogramowania.
Client-SMTP	Klienci SMTP	Wysyłają wiadomości e-mail bez wiedzy użytkownika. Hakerzy instalują je na komputerze użytkownika w celu wysłania spamu w jego imieniu.
WebToolbar	Paski narzędzi w przeglądarkach internetowych	Dodają one paski narzędzi w interfejsie innych aplikacji umożliwiające korzystanie z wyszukiwarek internetowych.
FraudTool	Pseudo-programy	Podają się za inne programy. Na przykład, istnieją fałszywe programy antywirusowe, które wyświetlają wiadomości o wykryciu szkodliwego oprogramowania. W rzeczywistości nie skanują ani nie leczą niczego.

- [Wykrywaj pozostałe programy, które mogą zostać wykorzystane przez przestępców do uszkodzenia komputera lub danych prywatnych](#) 

Podkategoria: legalne oprogramowanie, które może zostać wykorzystane przez cyberprzestępców do uszkodzenia komputera i prywatnych danych.

Poziom zagrożenia: średni

Wiele z tych programów to nieszkodliwe oprogramowanie, z którego korzysta wielu użytkowników. Do tych programów zaliczają się: klienci IRC, auto-dialery, programy pobierające pliki, monitory aktywności systemu komputerowego, narzędzia do haseł, serwery usług FTP, HTTP i Telnet.

Jednakże, jeśli haker uzyska dostęp do tego typu programów lub jeśli zainstaluje te programy na komputerze użytkownika, to niektóre z ich funkcji mogą zostać użyte do naruszenia ochrony.

Aplikacje te mają różne funkcje; ich typy zostały opisane w poniższej tabeli.

Typ	Nazwa	Opis
Client-IRC	Klienci czatów internetowych	Użytkownicy instalują programy tego typu, aby móc rozmawiać z innymi w czasie rzeczywistym. Hakerzy używają ich do rozsyłania szkodliwych programów.
Dialer	Auto-dialery	Mogą nawiązywać połączenie telefoniczne za pośrednictwem modemu w trybie ukrycia.
Downloader	Programy do pobierania	Mogą pobierać pliki ze stron internetowych w trybie ukrycia.
Monitor	Programy do monitorowania	Umożliwiają monitorowanie aktywności na komputerze, na którym są zainstalowane (sprawdzają, które aplikacje są aktywne i w jaki sposób wymieniają dane z aplikacjami zainstalowanymi na innych komputerach).
PSWTool	Programy do przywracania haseł	Umożliwiają przeglądanie i przywracanie zapomnianych haseł. Hakerzy umieszczają je na komputerze w tym samym celu, w sposób niezauważalny dla użytkownika.
RemoteAdmin	Programy do zdalnej administracji	Są używane przez administratorów systemów. Programy te pozwalają uzyskać dostęp do interfejsu zdalnego komputera w celu jego monitorowania i zarządzania. W tym właśnie celu hakerzy niezauważenie umieszczają je na komputerze użytkownika. Legalne programy do zdalnej administracji różnią się od trojanów typu backdoor do zdalnej administracji. Trojanzy potrafią niezależnie spenetrować system i zainstalować się; legalne programy nie potrafią tego.
Server-FTP	Serwery FTP	Działają jak serwery FTP. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu FTP.
Server-Proxy	Serwery proxy	Działają jak serwery proxy. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
Server-Telnet	Serwery Telnet	Działają jak serwery Telnet. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu Telnet.
Server-Web	Serwery sieciowe	Działają jak serwery sieciowe. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu HTTP.
RiskTool	Narzędzia	Umożliwiają one użytkownikowi korzystanie z dodatkowych

	wykorzystywane do pracy na lokalnym komputerze	funkcji podczas jego pracy na komputerze. Narzędzia te pozwalają użytkownikowi ukryć pliki lub okna uruchomionych aplikacji i zakończyć aktywne procesy.
NetTool	Narzędzia sieciowe	Umożliwiają użytkownikowi korzystanie z dodatkowych funkcji podczas pracy z innymi komputerami w sieci. Posiadają one także możliwość ich ponownego uruchomienia, wykrywania otwartych portów oraz uruchamiania aplikacji zainstalowanych na komputerach.
Client-P2P	Klienci sieciowe P2P	Pozwalają pracować w sieciach peer-to-peer. Mogą być wykorzystywane przez hakerów do rozprzestrzeniania szkodliwego oprogramowania.
Client-SMTP	Klienci SMTP	Wysyłają wiadomości e-mail bez wiedzy użytkownika. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
WebToolbar	Paski narzędzi w przeglądarkach internetowych	Dodają one paski narzędzi w interfejsie innych aplikacji umożliwiające korzystanie z wyszukiwarek internetowych.
FraudTool	Pseudo-programy	Podają się za inne programy. Na przykład, istnieją fałszywe programy antywirusowe, które wyświetlają wiadomości o wykryciu szkodliwego oprogramowania. W rzeczywistości nie skanują ani nie leczą niczego.

- [Obiekty spakowane, których archiwizacja może być używana do ochrony szkodliwego kodu](#)

Kaspersky Endpoint Security skanuje skompresowane obiekty i moduł wypakowujący znajdujące się w archiwach SFX (samorozpakowujących się).

Aby ukryć szkodliwe programy przed antywirusami, hakerzy archiwizują je przy pomocy dedykowanych narzędzi pakujących lub tworzą wielokrotnie spakowane obiekty.

Analitycy wirusów Kaspersky zidentyfikowali narzędzia pakujące najpopularniejsze wśród hakerów.

Jeśli Kaspersky Endpoint Security wykryje jeden z tych pakerów w pliku, plik ten najprawdopodobniej zawiera szkodliwą aplikację lub aplikację, która może zostać użyta przez cyberprzestępców do uszkodzenia komputera lub danych osobistych.

Kaspersky Endpoint Security wyróżnia następujące typy programów:

- *Spakowane pliki, które mogą wyrządzić szkody* – wykorzystywane do pakowania szkodliwego oprogramowania, takiego jak wirusy, robaki i trojany.
- *Pliki wielokrotnie spakowane* (średni poziom zagrożenia) – obiekt został spakowany trzy razy przez jedno lub więcej narzędzi pakujących.

- [Obiekty spakowane wielokrotnie](#)

Kaspersky Endpoint Security skanuje skompresowane obiekty i moduł wypakowujący znajdujące się w archiwach SFX (samorozpakowujących się).

Aby ukryć szkodliwe programy przed antywirusami, hakerzy archiwizują je przy pomocy dedykowanych narzędzi pakujących lub tworzą wielokrotnie spakowane obiekty.

Analitycy wirusów Kaspersky zidentyfikowali narzędzia pakujące najpopularniejsze wśród hakerów.

Jeśli Kaspersky Endpoint Security wykryje jeden z tych pakierów w pliku, plik ten najprawdopodobniej zawiera szkodliwą aplikację lub aplikację, która może zostać użyta przez cyberprzestępców do uszkodzenia komputera lub danych osobistych.

Kaspersky Endpoint Security wyróżnia następujące typy programów:

- *Spakowane pliki, które mogą wyrządzić szkody* – wykorzystywane do pakowania szkodliwego oprogramowania, takiego jak wirusy, robaki i trojany.
- *Pliki wielokrotnie spakowane* (średni poziom zagrożenia) – obiekt został spakowany trzy razy przez jedno lub więcej narzędzi pakujących.


4. Zapisz swoje zmiany.

Włączanie i wyłączanie technologii zaawansowanego leczenia

Jeśli program Kaspersky Endpoint Security nie może zatrzymać wykonania fragmentu szkodliwego oprogramowania, możesz użyć technologii zaawansowanego leczenia. Domyślnie, Zaawansowane leczenie jest wyłączone, ponieważ ta technologia używa znaczącej ilości zasobów komputera. Dlatego możesz włączyć Zaawansowane leczenie tylko wtedy, gdy [pracujesz z aktywnymi zagrożeniami](#).

Zaawansowane leczenie działa inaczej dla stacji roboczych i serwerów. Aby użyć technologii na serwerach, musisz [włączyć natychmiastowe zaawansowane leczenie](#) we właściwościach zadania *Skanowanie antywirusowe*. To wymaganie wstępne nie jest konieczne do używania technologii na stacjach roboczych.


W celu włączenia lub wyłączenia technologii zaawansowanego leczenia:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ogólne**.
3. W sekcji **Tryb działania** zaznacz lub odznacz pole **Włącz technologię zaawansowanego leczenia**, aby włączyć lub wyłączyć technologię zaawansowanego leczenia.
4. Zapisz swoje zmiany.

W trakcie przeprowadzania zaawansowanego leczenia użytkownik nie może korzystać z większości funkcji systemowych. Po zakończeniu leczenia, komputer zostaje uruchomiony ponownie.

Włączanie i wyłączanie trybu oszczędzania energii

W celu włączenia lub wyłączenia trybu oszczędzania energii:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz sekcję **Ustawienia zaawansowane** → **Zagrożenia i wykluczenia**.
3. W sekcji **Wydajność** użyj pola **Odrocz zaplanowane zadania podczas pracy na bateriach**, aby włączyć lub wyłączyć tryb oszczędzania energii.


Jeśli tryb oszczędzania energii jest włączony, a komputer działa na bateriach, następujące zadania nie są uruchamiane nawet wtedy, gdy skonfigurowano ich terminarz:

- Zadanie aktualizacji;
- Zadanie Pełne skanowanie;
- Zadanie Skanowanie obszarów krytycznych;
- Zadanie Skanowanie obiektów;
- Zadanie Sprawdzanie integralności.

4. Zapisz swoje zmiany.

Włączanie i wyłączanie udostępniania zasobów innym aplikacjom

W celu włączenia lub wyłączenia udostępniania zasobów innym aplikacjom:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ogólne**.
3. W sekcji **Wydajność** użyj pola **Współdziel zasoby z innymi aplikacjami**, aby włączyć lub wyłączyć współdzielenie zasobów z innymi aplikacjami.

Jeśli skonfigurowano udostępnianie zasobów innym aplikacjom, Kaspersky Endpoint Security odracza zaplanowane zadania, które mogą spowolnić inne aplikacje:

- Zadanie aktualizacji;
- Zadanie Pełne skanowanie;
- Zadanie Skanowanie obszarów krytycznych;
- Zadanie Skanowanie obiektów;
- Zadanie Sprawdzanie integralności.

Domyślnie aplikacja udostępnia zasoby innym aplikacjom.


4. Zapisz swoje zmiany.

Tworzenie i korzystanie z pliku konfiguracyjnego

Plik konfiguracyjny z ustawieniami Kaspersky Endpoint Security umożliwia wykonanie następujących zadań:

- Lokalnej instalacji Kaspersky Endpoint Security z predefiniowanymi ustawieniami z poziomu wiersza poleceń.
W tym celu należy zapisać plik konfiguracyjny w tym samym folderze, w którym znajduje się pakiet dystrybucyjny.
- Zdalnej instalacji Kaspersky Endpoint Security z predefiniowanymi ustawieniami z poziomu Kaspersky Security Center.
- Przeniesienie ustawień Kaspersky Endpoint Security z jednego komputera na drugi.


W celu utworzenia pliku konfiguracyjnego:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Zarządzaj ustawieniami**.
3. Kliknij przycisk **Eksportuj**.
4. W otwartym oknie wskaż miejsce, w którym chcesz zapisać plik konfiguracyjny, i wprowadź nazwę pliku.

Aby użyć pliku konfiguracyjnego dla lokalnej lub zdalnej instalacji Kaspersky Endpoint Security, należy wpisać nazwę `install.cfg`.

5. Kliknij przycisk **Zapisz**.

W celu zaimportowania ustawień Kaspersky Endpoint Security z pliku konfiguracyjnego:


1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Zarządzaj ustawieniami**.
3. Kliknij przycisk **Importuj**.
4. W otwartym oknie wprowadź ścieżkę dostępu do pliku konfiguracyjnego.
5. Kliknij przycisk **Otwórz**.

Wszystkie wartości ustawień Kaspersky Endpoint Security zostaną ustawione zgodnie z wybranym plikiem konfiguracyjnym.

Przywracanie ustawień domyślnych aplikacji

W każdej chwili możesz przywrócić ustawienia zalecane przez firmę Kaspersky dla Endpoint Security. Po przywróceniu ustawień, poziom ochrony wszystkich modułów zostaje ustawiony na **Zalecany**.

W celu przywrócenia domyślnych ustawień aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Zarządzaj ustawieniami**.
3. Kliknij przycisk **Przywróć**.
4. Zapisz swoje zmiany.

Przesyłanie wiadomości między użytkownikami a administratorem

Komponenty [Kontrola aplikacji](#), [Kontrola urządzeń](#), [Kontrola sieci](#) i [Adaptacyjna kontrola anomalii](#) umożliwiają użytkownikom sieci LAN, którzy mają zainstalowany program Kaspersky Endpoint Security, wysyłanie wiadomości do administratora.

Użytkownik może chcieć wysłać wiadomość do administratora lokalnej sieci firmowej w następujących przypadkach:

- Kontrola urządzeń zablokowała dostęp do urządzenia.
Szablon wiadomości z prośbą o dostęp do zablokowanego urządzenia jest dostępny w interfejsie Kaspersky Endpoint Security, w sekcji [Kontrola urządzeń](#).
- Kontrola aplikacji zablokowała uruchomienie aplikacji.
Szablon wiadomości z prośbą o zezwolenie na uruchomienie zablokowanej aplikacji jest dostępny w interfejsie Kaspersky Endpoint Security, w sekcji [Kontrola aplikacji](#).
- Kontrola sieci zablokowała dostęp do zasobu sieciowego.
Szablon wiadomości z prośbą o dostęp do zablokowanego zasobu sieciowego jest dostępny w interfejsie Kaspersky Endpoint Security, w sekcji [Kontrola sieci](#).

Metoda używana do wysyłania wiadomości oraz wykorzystanie szablonu zależą od tego, czy na komputerze z zainstalowanym programem Kaspersky Endpoint Security działa profil Kaspersky Security Center oraz czy jest połączenie z Serwerem administracyjnym Kaspersky Security Center. Możliwe są następujące scenariusze:

- Jeśli profil Kaspersky Security Center nie działa na komputerze, na którym jest zainstalowany Kaspersky Endpoint Security, komunikat użytkownika zostanie wysłany do administratora sieci lokalnej za pośrednictwem poczty elektronicznej.
Pola wiadomości są uzupełniane wartościami z pól szablonu, zdefiniowanego w lokalnym interfejsie Kaspersky Endpoint Security.
- Jeśli profil Kaspersky Security Center działa na komputerze, na którym jest zainstalowany Kaspersky Endpoint Security, standardowa wiadomość zostanie wysłana na Serwer administracyjny Kaspersky Security Center.
W tym przypadku wiadomości użytkownika można sprawdzić w miejscu przechowywania zdarzeń programu Kaspersky Security Center (patrz instrukcja poniżej). Pola wiadomości są uzupełniane wartościami z szablonu zdefiniowanego w profilu Kaspersky Security Center.
- Jeśli na komputerze z zainstalowanym produktem Kaspersky Endpoint Security działa profil użytkownika mobilnego z Kaspersky Security Center, metoda używana do wysyłania wiadomości zależy od tego, czy jest połączenie z Kaspersky Security Center.
 - Jeśli zostało nawiązane połączenie z Kaspersky Security Center, Kaspersky Endpoint Security wysyła standardową wiadomość na Serwer administracyjny Kaspersky Security Center.
 - Jeśli nie zostało nawiązane połączenie z Kaspersky Security Center, komunikat użytkownika jest wysyłany do administratora sieci lokalnej za pośrednictwem poczty elektronicznej.

W obu przypadkach pola wiadomości są uzupełniane wartościami z szablonu zdefiniowanego w profilu Kaspersky Security Center.

W celu przejrzenia wiadomości użytkownika w miejscu przechowywania zdarzeń programu Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Zdarzenia**.

Obszar roboczy Kaspersky Security Center wyświetla wszystkie zdarzenia występujące podczas działania Kaspersky Endpoint Security, w tym wiadomości wysyłane do administratora, które są odbierane przez użytkowników sieci LAN.

3. Aby skonfigurować filtrowanie zdarzeń, na liście rozwijalnej **Wybory zdarzeń** wybierz **Żądania użytkownika**.
4. Wybierz wiadomość, która ma zostać wysłana do administratora.
5. W prawej części obszaru roboczego Konsoli administracyjnej kliknij **Otwórz okno właściwości zdarzenia**.

Szyfrowanie danych

Kaspersky Endpoint Security umożliwia szyfrowanie plików i folderów przechowywanych na dyskach lokalnych i nośnikach wymiennych lub wszystkich nośnikach wymiennych i dyskach twardej. Szyfrowanie danych minimalizuje ryzyko wycieku informacji, co może mieć miejsce, gdy komputer przenośny, nośnik wymienny lub dysk twardy zostanie zgubiony bądź skradziony lub gdy dostęp do danych jest uzyskiwany przez nieautoryzowanych użytkowników lub aplikacje. Kaspersky Endpoint Security używa algorytmu szyfrowania AES (Advanced Encryption Standard).

Jeśli licencja wygasła, aplikacja nie szyfruje nowych danych, a stare zaszyfrowane dane pozostają zaszyfrowane i dostępne do użycia. W tej sytuacji szyfrowanie nowych danych wymaga aktywacji aplikacji z nową licencją zezwalającą na korzystanie z szyfrowania.

Jeśli licencja utraciła ważność, postanowienia Umowy licencyjnej zostały naruszone lub klucz licencyjny, program Kaspersky Endpoint Security bądź moduły szyfrujące zostały usunięte, stan zaszyfrowany wcześniej zaszyfrowanych plików nie zostanie zagwarantowany. Dzieje się tak, ponieważ niektóre aplikacje, takie jak Microsoft Office Word, podczas modyfikacji tworzą tymczasowe kopie plików. Po zapisaniu oryginalnego pliku, tymczasowa kopia zastępuje oryginalny plik. W rezultacie, na komputerze, na którym nie ma żadnej lub dostępnej funkcji szyfrowania, plik pozostanie niezaszyfrowany.

Kaspersky Endpoint Security oferuje następujące aspekty ochrony danych:

- **Szyfrowanie na poziomie plików na lokalnych dyskach komputera.** Możesz [tworzyć listy plików](#) według rozszerzenia lub grup rozszerzeń oraz listy folderów przechowywanych na lokalnych dyskach komputera, a także tworzyć [reguły szyfrowania plików, które są tworzone przez określone aplikacje](#). Po zastosowaniu zasady, Kaspersky Endpoint Security zaszyfruje i odszyfruje następujące pliki:
 - Pliki pojedynczo dodane do list elementów przeznaczonych do zaszyfrowania i odszyfrowania;
 - Pliki przechowywane w folderach dodanych do list elementów przeznaczonych do zaszyfrowania i odszyfrowania;
 - Pliki utworzone przez oddzielne aplikacje.
- **Szyfrowanie dysków wymiennych.** Możesz określić domyślną regułę szyfrowania, zgodnie z którą aplikacja stosuje tę samą akcję do wszystkich dysków wymiennych lub określić reguły szyfrowania dla pojedynczych dysków wymiennych.

Domyślna reguła szyfrowania ma niższy priorytet niż reguły szyfrowania utworzone dla pojedynczych dysków wymiennych. Reguły szyfrowania utworzone dla dysków wymiennych z określonym modelem urządzenia mają niższy priorytet niż reguły szyfrowania, utworzone dla dysków wymiennych z określonym kodem ID urządzenia.

Aby wybrać regułę szyfrowania dla plików na nośniku wymiennym, Kaspersky Endpoint Security sprawdza, czy model i kod ID urządzenia są znane. Następnie aplikacja wykonuje jedną z poniższych czynności:

- Jeśli tylko model urządzenia jest znany, aplikacja używa reguły szyfrowania (jeśli istnieje), utworzonej dla dysków wymiennych o określonym modelu urządzenia.
- Jeśli tylko ID urządzenia jest znane, aplikacja używa reguły szyfrowania (jeśli istnieje), utworzonej dla dysków wymiennych o określonym ID urządzenia.
- Jeśli model i ID urządzenia są znane, aplikacja stosuje regułę szyfrowania (jeśli istnieje), utworzoną dla dysków wymiennych o określonym ID urządzenia. Jeśli nie istnieje taka reguła, ale istnieje reguła szyfrowania utworzona dla nośników wymiennych o określonym modelu urządzenia, aplikacja zastosuje tę regułę. Jeśli dla określonego ID urządzenia i określonego modelu urządzenia nie określono żadnej reguły szyfrowania, aplikacja zastosuje domyślną regułę szyfrowania.

- Jeśli nie jest znany model i kod ID urządzenia, aplikacja używa domyślnej reguły szyfrowania.

Aplikacja umożliwia przygotowanie dysku wymiennego do używania w trybie przenośnym przechowywanych na nim zaszyfrowanych danych. Po włączeniu trybu przenośnego, użytkownik może uzyskać dostęp do zaszyfrowanych plików na dyskach wymiennych podłączonych do komputera bez funkcji szyfrowania.

- **Zarządzanie regułami dostępu aplikacji do zaszyfrowanych plików.** Dla dowolnej aplikacji użytkownik może utworzyć regułę dostępu do zaszyfrowanego pliku, która zablokuje dostęp do zaszyfrowanych plików lub zezwoli na dostęp do zaszyfrowanych plików tylko jako tekst zaszyfrowany, który jest sekwencją znaków uzyskanych w momencie stosowania szyfrowania.
- **Tworzenie zaszyfrowanych pakietów.** Możesz utworzyć zaszyfrowane archiwa i chronić dostęp do takich archiwów przy pomocy hasła. Dostęp do zawartości zaszyfrowanych archiwów można uzyskać tylko poprzez wprowadzenie haseł, przy pomocy których chroniony jest dostęp do tych archiwów. Takie archiwa można bezpiecznie przesyłać poprzez sieci lub nośniki wymienne.
- **Szyfrowanie całego dysku.** Możesz wybrać technologię szyfrowania: Kaspersky Disk Encryption lub Szyfrowanie dysków funkcją BitLocker (zwana dalej również "BitLocker").

BitLocker to technologia, która jest częścią systemu operacyjnego Windows. Jeśli komputer zawiera moduł Trusted Platform Module (TPM), BitLocker używa go do przechowywania kluczy dostępu, które umożliwiają uzyskanie dostępu do zaszyfrowanego dysku twardego. Po uruchomieniu komputera, BitLocker żąda od Trusted Platform Module kluczy odzyskiwania dysku twardego i odblokowuje dysk. Możesz skonfigurować korzystanie z hasła i/lub kodu PIN do uzyskania dostępu do kluczy odzyskiwania.

Możesz określić domyślną regułę szyfrowania całego dysku oraz utworzyć listę dysków twardech wykluczonych z szyfrowania. Po zastosowaniu profilu Kaspersky Security Center, program Kaspersky Endpoint Security zaszyfruje cały dysk sektor po sektorze. Aplikacja szyfruje wszystkie logiczne partycje dysków twardech jednocześnie.

Po zaszyfrowaniu dysków twardech, przy kolejnym uruchomieniu komputera użytkownik musi przejść proces autoryzacji przy użyciu [Agenta autoryzacji](#) przed uzyskaniem dostępu do dysków twardech i załadowaniem systemu operacyjnego. Wymaga to wprowadzenia hasła do tokena lub karty inteligentnej podłączonej do komputera, bądź wpisania nazwy użytkownika i hasła konta Agentu autoryzacji utworzonego przez administratora lokalnej sieci firmowej przy użyciu zadania [Zarządzanie kontem Agentu autoryzacji](#). Konta te są oparte na kontach systemu Microsoft Windows, z poziomu których użytkownik loguje się do systemu operacyjnego. Możesz także [użyć technologii logowania jednokrotnego \(SSO\)](#), która umożliwia automatyczne logowanie do systemu operacyjnego przy użyciu nazwy użytkownika i hasła dla konta Agentu autoryzacji.

Jeśli utworzysz kopie zapasowe danych komputera, a następnie zaszyfrujesz dane komputera, po czym przywrócisz kopie zapasowe danych komputera i ponownie zaszyfrujesz dane komputera, Kaspersky Endpoint Security utworzy kopie kont Agentu autoryzacji. Aby usunąć kopie kont, użyj narzędzia klmover z parametrem `dupfix`. Narzędzie klmover jest dostępne z programem Kaspersky Security Center. Więcej na temat działania tego narzędzia można znaleźć w systemie pomocy programu Kaspersky Security Center.

Dostęp do zaszyfrowanych dysków twardech jest możliwy tylko z poziomu komputerów, na których zainstalowany jest program Kaspersky Endpoint Security z funkcją szyfrowania całego dysku. Ten środek bezpieczeństwa minimalizuje ryzyko wycieku danych z zaszyfrowanego dysku twardego, gdy podjęta zostaje próba uzyskania dostępu do tego dysku spoza lokalnej sieci firmowej.

Aby zaszyfrować dyski twarde i nośniki wymienne, możesz użyć funkcji **Zaszyfruj tylko używaną przestrzeń dyskową**. Zalecane jest korzystanie z tej funkcji tylko w przypadku nowych urządzeń, które nie były wcześniej używane. Jeśli stosujesz szyfrowanie do urządzenia, które jest już w użyciu, zalecane jest zaszyfrowanie całego urządzenia. Zapewni to ochronę wszystkich danych, także tych usuniętych, gdyż mogą zawierać informacje, które można odzyskać.

Przed rozpoczęciem szyfrowania program Kaspersky Endpoint Security uzyskuje mapę sektorów systemu plików. Pierwszy etap szyfrowania obejmuje sektory zajmowane przez pliki w momencie rozpoczęcia szyfrowania. Drugi etap szyfrowania obejmuje sektory zapisane po rozpoczęciu szyfrowania. Po zakończeniu szyfrowania, wszystkie sektory zawierające dane zostają zaszyfrowane.

Po zakończeniu szyfrowania i usunięciu pliku przez użytkownika, sektory, w których był przechowywany usunięty plik, staną się niedostępne do przechowywania nowych informacji na poziomie systemu plików, ale pozostaną zaszyfrowane. Dlatego też, jeśli pliki są zapisywane na nowym urządzeniu, a urządzenie jest regularnie szyfrowane przy użyciu włączonej funkcji **Zaszyfruj tylko używaną przestrzeń dyskową**, wszystkie sektory zostaną zaszyfrowane po jakimś czasie.

Dane potrzebne do odszyfrowania plików są udostępniane przez Serwer administracyjny Kaspersky Security Center, który kontrolował komputer w momencie szyfrowania. Jeśli komputer z zaszyfrowanymi obiektami był z jakiegoś powodu zarządzany przez inny Serwer administracyjny, możesz uzyskać dostęp do zaszyfrowanych danych na jeden z następujących sposobów:

- Serwery administracyjne w tej samej hierarchii:
 - Nie musisz podejmować żadnych dodatkowych działań. Użytkownik zachowa dostęp do zaszyfrowanych obiektów. Klucze szyfrujące są dystrybuowane do wszystkich Serwerów administracyjnych.
- Oddzielne Serwery administracyjne:
 - Wyślij prośbę do administratora sieci LAN o dostęp do zaszyfrowanych obiektów.
 - Przywróć dane na zaszyfrowanych urządzeniach przy użyciu Narzędzia przywracania.
 - Przywróć z kopii zapasowej konfigurację Serwera administracyjnego Kaspersky Security Center kontrolującego komputer w momencie szyfrowania i użyj tej konfiguracji na Serwerze administracyjnym obecnie kontrolującym komputer z zaszyfrowanymi obiektami.

Jeśli nie ma dostępu do zaszyfrowanych danych, postępuj zgodnie ze specjalnymi instrukcjami dotyczącymi pracy z zaszyfrowanymi danymi ([Przywracanie dostępu do zaszyfrowanych plików](#), [Praca z zaszyfrowanymi urządzeniami, gdy nie ma do nich dostępu](#)).

Ograniczenia funkcji szyfrowania

Szyfrowanie danych posiada następujące ograniczenia:

- Podczas szyfrowania aplikacja tworzy pliki usługi. Do ich przechowywania potrzeba około 0,5 % niepofragmentowanej, wolnej przestrzeni na dysku. Jeśli na dysku twardym nie ma wystarczającej ilości niepofragmentowanego, wolnego miejsca, szyfrowanie nie zostanie rozpoczęte, aż do zwolnienia wystarczającej ilości miejsca.
- Zarządzanie komponentami szyfrującymi wszystkie dane jest dostępne w Konsoli administracyjnej Kaspersky Security Center i w konsoli Kaspersky Security Center Web Console. W konsoli Kaspersky Security Center Cloud Console możesz tylko zarządzać Bitlocker.
- Szyfrowanie danych jest dostępne tylko podczas używania Kaspersky Endpoint Security z systemem zarządzania Kaspersky Security Center lub Kaspersky Security Center Cloud Console (tylko BitLocker). Szyfrowanie danych podczas korzystania z Kaspersky Endpoint Security w trybie offline nie jest możliwe, ponieważ Kaspersky Endpoint Security przechowuje klucze szyfrowania w Kaspersky Security Center.
- Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu [Microsoft Windows dla serwerów](#), dostępne jest tylko szyfrowanie całego dysku przy użyciu technologii

Szyfrowanie dysków funkcją BitLocker. Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych, funkcja szyfrowania danych jest w pełni dostępna.

Szyfrowanie całego dysku przy użyciu technologii Kaspersky Disk Encryption jest niedostępne dla dysków twardek, które nie spełniają wymagań sprzętowych i programowych.

Kompatybilność funkcji szyfrowania całego dysku Kaspersky Endpoint Security z Kaspersky Anti-Virus dla UEFI nie jest obsługiwana. Kaspersky Anti-Virus dla UEFI uruchamia się przed załadowaniem systemu operacyjnego. Podczas korzystania z szyfrowania całego dysku aplikacja wykryje brak zainstalowanego systemu operacyjnego na komputerze. W rezultacie działanie Kaspersky Anti-Virus dla UEFI zakończy się błędem. Szyfrowanie na poziomie plików (FLE) nie wpływa na działanie programu Kaspersky Anti-Virus dla UEFI.

Kaspersky Endpoint Security obsługuje następujące konfiguracje:

- Dyski HDD, SSD i USB.

Technologia Kaspersky Disk Encryption (FDE) obsługuje pracę z dyskami SSD, zapewniając działanie i okres użytkowania dysków SSD.

- Dyski podłączone poprzez magistralę: SCSI, ATA, IEEE1394, USB, RAID, SAS, SATA, NVME.
- Dyski niewymienne podłączone poprzez magistralę SD lub MMC.
- Dyski z sektorami o pojemności 512 bajtów.
- Dyski z sektorami o pojemności 4096 bajtów, które emulują 512 bajtów.
- Dyski z następującym typem partycji: GPT, MBR i VBR (dyski wymienne).
- Wbudowane oprogramowanie ze standardem UEFI 64 i Legacy BIOS.
- Wbudowane oprogramowanie ze standardem UEFI z obsługą Bezpiecznego rozruchu.

Bezpieczny rozruch to technologia zaprojektowana do zweryfikowania podpisów cyfrowych dla sterowników i aplikacji UEFI loader. Bezpieczny rozruch blokuje uruchamianie sterowników i aplikacji w środowisku UEFI, które nie są podpisane lub są podpisane przez nieznanych wydawców. Kaspersky Disk Encryption (FDE) w pełni obsługuje Bezpieczny rozruch. Agent autoryzacji jest podpisany certyfikatem Microsoft Windows UEFI Driver Publisher.

Na niektórych urządzeniach (na przykład: Microsoft Surface Pro i Microsoft Surface Pro 2), domyślnie zainstalowana może być przestarzała lista certyfikatów weryfikacji podpisów cyfrowych. Przed zaszyfrowaniem sterownika należy zaktualizować listę certyfikatów.

- Wbudowane oprogramowanie ze standardem UEFI z obsługą opcji Fast Boot.

Fast Boot to technologia, która pomaga w szybszym uruchomieniu komputera. Jeśli technologia Fast Boot jest włączona, zazwyczaj komputer ładuje tylko minimalny zestaw sterowników UEFI wymaganych do uruchomienia systemu operacyjnego. Jeśli technologia Fast Boot jest włączona, klawiatury USB, mysz, tokeny USB, touchpady i ekrany dotykowe mogą nie działać, gdy uruchomiony jest Agent autoryzacji.

Aby użyć Kaspersky Disk Encryption (FDE), zalecane jest wyłączenie technologii Fast Boot. Aby sprawdzić działanie Kaspersky Disk Encryption (FDE), możesz użyć narzędzia [FDE Test Utility](#).

Kaspersky Endpoint Security nie obsługuje następujących konfiguracji:

- Moduł ładujący rozruch znajduje się na jednym dysku, a system operacyjny na innym dysku.
- System zawiera oprogramowanie wbudowane w standardzie UEFI 32.
- System posiada technologię Intel® Rapid Start Technology i dyski, które posiadają partycję hibernacji nawet wtedy, gdy technologia Intel® Rapid Start Technology jest wyłączona.
- Dyski w formacie MBR z więcej niż 10 partycjami rozszerzonymi.
- System zawiera plik wymiany znajdujący się na dysku niesystemowym.
- Możliwość uruchamiania wielu systemów operacyjnych na komputerze z kilkoma jednocześnie zainstalowanymi systemami operacyjnymi.
- Partycje dynamiczne (obsługiwane są tylko główne partycje).
- Dyski posiadające mniej niż 0,5% wolnej niepofragmentowanej przestrzeni.
- Dyski posiadające sektor o rozmiarze innym niż 512 bajtów lub 4096 bajtów, który emuluje 512 bajtów.
- Dyski hybrydowe.
- System posiada moduły ładujące innych firm.
- Dyski ze skompresowanymi katalogami NTFS.
- Technologia Kaspersky Disk Encryption (FDE) jest niekompatybilna z innymi technologiami szyfrowania całego dysku (takimi, jak: BitLocker, McAfee Drive Encryption i WinMagic SecureDoc).
- Technologia Kaspersky Disk Encryption (FDE) jest niekompatybilna z technologią Express Cache.
- Tworzenie, usuwanie i modyfikowanie partycji na dysku zaszyfrowanym nie jest obsługiwane. Mógłbyś utracić dane.
- Formatowanie systemu plików nie jest obsługiwane. Mógłbyś utracić dane.
 Jeśli chcesz sformatować dysk, który został zaszyfrowany przy pomocy technologii Kaspersky Disk Encryption (FDE), sformatuj dysk na komputerze, na którym nie ma programu Kaspersky Endpoint Security for Windows, i użyj tylko szyfrowania całego dysku.
 Zaszyfrowany dysk, który jest formatowany przy użyciu opcji szybkiego formatowania, przy następnym podłączeniu do komputera z zainstalowanym programem Kaspersky Endpoint Security for Windows może być błędnie identyfikowany jako zaszyfrowany. Dane użytkownika będą niedostępne.
- Agent autoryzacji obsługuje nie więcej niż 100 kont.
- Technologia logowania jednokrotnego (SSO) jest niekompatybilna z innymi technologiami deweloperów innych firm.
- Technologia Kaspersky Disk Encryption (FDE) nie jest obsługiwana na następujących modelach urządzeń:
 - Dell Latitude E6410 (tryb UEFI)
 - HP Compaq nc8430 (tryb Legacy BIOS)
 - Lenovo Think Center 8811 (tryb Legacy BIOS)

- Agent autoryzacji nie obsługuje pracy z tokenami USB po włączeniu obsługi starszych wersji USB. Na komputerze możliwe będzie tylko uwierzytelnianie przy użyciu hasła.
- Podczas szyfrowania dysku w trybie Legacy BIOS zalecane jest włączenie obsługi starszych wersji USB na następujących modelach urządzeń:
 - Acer Aspire 5560G
 - Acer Aspire 6930
 - Acer TravelMate 8572T
 - Dell Inspiron 1420
 - Dell Inspiron 1545
 - Dell Inspiron 1750
 - Dell Inspiron N4110
 - Dell Latitude E4300
 - Dell Studio 1537
 - Dell Studio 1569
 - Dell Vostro 1310
 - Dell Vostro 1320
 - Dell Vostro 1510
 - Dell Vostro 1720
 - Dell Vostro V13
 - Dell XPS L502x
 - Fujitsu Celsius W370
 - Fujitsu LifeBook A555
 - HP Compaq dx2450 Microtower PC
 - Lenovo G550
 - Lenovo ThinkPad L530
 - Lenovo ThinkPad T510
 - Lenovo ThinkPad W540
 - Lenovo ThinkPad X121e
 - Lenovo ThinkPad X200s (74665YG)

- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 100
- MSI 760GM-E51 (płyta główna)

Zmiana długości klucza szyfrowania (AES56 / AES256)

Kaspersky Endpoint Security używa algorytmu szyfrowania AES (Advanced Encryption Standard). Kaspersky Endpoint Security obsługuje algorytm szyfrowania AES o efektywnej długości klucza 256 lub 56 bitów. Algorytm szyfrowania danych zależy od biblioteki szyfrowania AES zawartej w pakiecie dystrybucyjnym: *Silne szyfrowanie (AES256)* lub *Uprozczone szyfrowanie (AES56)*. Biblioteka szyfrowania AES jest instalowana wraz z aplikacją.

Zmiana długości klucza szyfrowania jest dostępna tylko dla Kaspersky Endpoint Security 11.2.0 lub nowszego.

Zmiana długości klucza szyfrowania składa się z następujących kroków:

1. Przed zmianą długości klucza szyfrowania odszyfruj obiekty, które Kaspersky Endpoint Security zaszyfrował.
 - a. [Odszyfruj dyski twarde.](#)
 - b. [Odszyfruj pliki na dyskach lokalnych.](#)
 - c. [Odszyfruj nośniki wymienne.](#)

Po zmianie długości klucza szyfrowania, obiekty, które zostały wcześniej zaszyfrowane, staną się niedostępne.

2. [Usuń Kaspersky Endpoint Security.](#)
3. [Zainstaluj Kaspersky Endpoint Security](#) z pakietu dystrybucyjnego Kaspersky Endpoint Security zawierającego inną bibliotekę szyfrowania.

Możesz także zmienić długość klucza szyfrowania, aktualizując aplikację. Długość klucza można zmienić poprzez aktualizację aplikacji tylko wtedy, gdy spełnione są następujące warunki:

- Kaspersky Endpoint Security w wersji 10 z dodatkiem Service Pack 2 lub nowszym jest zainstalowany na komputerze.
- Komponenty szyfrowania danych (Szyfrowanie plików, Szyfrowanie całego dysku) nie są zainstalowane na komputerze.

Domyślnie komponenty szyfrowania danych nie są zawarte w Kaspersky Endpoint Security. Komponent Zarządzanie BitLocker nie wpływa na zmianę długości klucza szyfrowania.

Aby zmienić długość klucza szyfrowania, uruchom plik kes_win.msi lub setup_kes.exe z pakietu dystrybucyjnego zawierającego niezbędną bibliotekę szyfrowania. Możesz także zdalnie zaktualizować aplikację za pomocą pakietu instalacyjnego.

Nie można zmienić długości klucza szyfrowania za pomocą pakietu dystrybucyjnego tej samej wersji aplikacji, która jest zainstalowana na komputerze bez uprzedniego odinstalowania aplikacji.

Kaspersky Disk Encryption

Kaspersky Disk Encryption jest dostępny tylko dla komputerów z systemem operacyjnym Windows dla stacji roboczych. W przypadku komputerów z systemem operacyjnym Windows dla serwerów użyj technologii szyfrowania dysków funkcją BitLocker.

Kaspersky Endpoint Security obsługuje szyfrowanie całego dysku z systemami plików FAT32, NTFS i exFat.

Przed rozpoczęciem szyfrowania całego dysku aplikacja przeprowadza serie skanowań (np. sprawdza dysk twardy systemu na kompatybilność z Agentem autoryzacji i komponentami technologii BitLocker) w celu określenia, czy urządzenie może zostać zaszyfrowane. Aby sprawdzenie kompatybilności mogło się odbyć, należy uruchomić ponownie komputer. Po ponownym uruchomieniu komputera aplikacja automatycznie przeprowadzi wszystkie potrzebne skanowania. Jeśli sprawdzenie kompatybilności zostanie zakończone pomyślnie, szyfrowanie całego dysku rozpocznie się po załadowaniu systemu operacyjnego i uruchomieniu aplikacji. Jeśli skanowanie wykaże niekompatybilność dysku twardego z Agentem autoryzacji lub komponentami technologii BitLocker, komputer będzie musiał zostać uruchomiony ponownie przez wciśnięcie przycisku restartu sprzętowego. Kaspersky Endpoint Security zapisuje informacje o niekompatybilności. W oparciu o te informacje aplikacja nie uruchamia szyfrowania całego dysku przy uruchamianiu systemu operacyjnego. Informacja o tym zdarzeniu jest zapisywana w raporcie Kaspersky Security Center.

Jeśli konfiguracja sprzętowa komputera została zmieniona, informacje o niekompatybilności, zapisane przez aplikację podczas poprzedniego skanowania, powinny zostać usunięte w celu sprawdzenia dysku twardego na kompatybilność z Agentem autoryzacji i komponentami technologii BitLocker. W tym celu, przed zaszyfrowaniem całego dysku, w wierszu polecenia wpisz `avp pbatestreset`. Jeśli system operacyjny nie ładuje się po sprawdzeniu dysku twardego na kompatybilność z Agentem autoryzacji, [usuń obiekty i dane pozostałe po testowym działaniu Agenta autoryzacji](#), korzystając z Narzędzia przywracania zaszyfrowanego urządzenia. Następnie uruchom Kaspersky Endpoint Security i ponownie wykonaj polecenie `avp pbatestreset`.

Po uruchomieniu szyfrowania całego dysku, Kaspersky Endpoint Security zaszyfruje wszystkie dane zapisane na dyskach twardech.

Jeśli podczas szyfrowania całego dysku użytkownik zamknie lub uruchomi ponownie komputer, Agent autoryzacji ładuje się przed kolejnym uruchomieniem systemu operacyjnego. Kaspersky Endpoint Security wznawia szyfrowanie całego dysku po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego.

Jeśli podczas szyfrowania całego dysku system operacyjny przełączy się w tryb hibernacji, Agent autoryzacji zostanie załadowany po wyjściu systemu operacyjnego z trybu hibernacji. Kaspersky Endpoint Security wznawia szyfrowanie całego dysku po pomyślnej autoryzacji w Agencie autoryzacji i uruchomieniu systemu operacyjnego.

Jeśli podczas szyfrowania całego dysku system operacyjny przejdzie w tryb uśpienia, Kaspersky Endpoint Security wznowi szyfrowanie całego dysku po wyjściu systemu operacyjnego z trybu uśpienia, bez wczytywania Agenta autoryzacji.

Autoryzacja użytkownika w Agencie autoryzacji może przebiegać na dwa sposoby:

- Poprzez wprowadzenie nazwy i hasła konta Agenta autoryzacji, utworzonego przez administratora sieci LAN przy użyciu narzędzi Kaspersky Security Center.

- Poprzez wprowadzenie hasła do tokena lub karty inteligentnej, podłączonych do komputera.

Użycie tokena lub karty inteligentnej jest możliwe tylko wtedy, gdy dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES256. Jeśli dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES56, dodanie pliku certyfikatu elektronicznego do polecenia zostanie odrzucone.

Agent autoryzacji obsługuje układy klawiatury dla następujących języków:

- Angielski (UK)
- Angielski (USA)
- Arabski (Algieria, Maroko, Tunis; układ AZERTY)
- Hiszpański (Ameryka Łacińska)
- Włoski
- Niemiecki (Niemcy i Austria)
- Niemiecki (Szwajcaria)
- Portugalski (Brazylia, układ ABNT2)
- Rosyjski (dla klawiatury o 105 klawiszach odpowiadającej układowi QWERTY systemu IBM / Windows)
- Turecki (układ QWERTY)
- Francuski (Francja)
- Francuski (Szwajcaria)
- Francuski (Belgia, układ AZERTY)
- Japoński (dla klawiatury o 106 klawiszach z układem QWERTY)

Układ klawiatury staje się dostępny w Agencji autoryzacji, jeśli ten układ został dodany w ustawieniach języka i standardów regionalnych systemu operacyjnego oraz stał się dostępny na ekranie powitalnym Microsoft Windows.

Jeśli nazwa konta Agenta autoryzacji zawiera symbole, których nie można wprowadzić przy użyciu układów klawiatury dostępnych w Agencji autoryzacji, dostęp do zaszyfrowanych dysków twardech można uzyskać tylko po ich przywróceniu przy pomocy Narzędzia przywracania zaszyfrowanego urządzenia lub po [odzyskaniu nazwy i hasła konta Agenta autoryzacji](#).

Specjalne funkcje szyfrowania dysku SSD

Aplikacja obsługuje szyfrowanie dysków SSD, hybryd dysków SSHD i dysków z funkcją Intel Smart Response. Aplikacja nie obsługuje szyfrowania dysków z funkcją Intel Rapid Start. Przed zaszyfrowaniem tego dysku wyłącz funkcję Intel Rapid Start.

Szyfrowanie dysków SSD ma następujące funkcje specjalne:

- Jeśli dysk SSD jest nowy i nie zawiera poufnych danych, [włącz szyfrowanie tylko zajętego obszaru](#). To umożliwia nadpisanie odpowiednich sektorów dysku.
- Jeśli używany jest dysk SSD i zawiera poufne dane, wybierz jedną z następujących opcji:
 - Całkowicie wyczyść dysk SSD (Secure Erase), zainstaluj system operacyjny i [uruchom szyfrowanie dysku SSD z wyłączoną opcją do szyfrowania tylko zajętego obszaru](#).
 - Uruchom szyfrowanie dysku SSD z wyłączoną opcją szyfrowania tylko zajętego obszaru.

Szyfrowanie dysku SSD wymaga 5-10 GB wolnego miejsca. Wymagania wolnej przestrzeni do przechowywania danych administracyjnych szyfrowania są dostępne w poniższej tabeli.

Wymagania wolnej przestrzeni do przechowywania danych administracyjnych szyfrowania

Rozmiar dysku SSD (GB)	Wolna przestrzeń na głównej partycji dysku SSD (MB)	Wolna przestrzeń na drugiej partycji dysku SSD (MB)
128	250	64
256	250	640
512	300	128

Szyfrowanie całego dysku przy użyciu technologii Kaspersky Disk Encryption

Przed uruchomieniem szyfrowania całego dysku zalecane jest upewnienie się, że komputer nie jest zainfekowany. W tym celu uruchom zadanie Pełne skanowanie lub Skanowanie obszarów krytycznych. Wykonanie szyfrowania całego dysku na komputerze, który jest zainfekowany rootkitem, może spowodować, że komputer przestanie działać.

W celu uruchomienia szyfrowania całego dysku przy użyciu technologii Kaspersky Disk Encryption:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
6. Z listy rozwijalnej **Technologia szyfrowania** wybierz opcję **Kaspersky Disk Encryption**.

Technologia Kaspersky Disk Encryption nie może być użyta, jeśli dyski twarde komputera zostały zaszyfrowane przy użyciu funkcji BitLocker.

7. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zaszyfruj wszystkie dyski twarde**.

Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po zaszyfrowaniu wszystkich dysków twardych będziesz mógł załadować tylko ten system operacyjny, na którym jest zainstalowana aplikacja.

Jeśli chcesz wykluczyć niektóre dyski twarde z szyfrowania, [utwórz listę tych dysków twardych](#).

8. Konfiguruj reguły dodawania kont Agenta autoryzacji podczas szyfrowania dysku. Agent umożliwia użytkownikowi zakończenie autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków i do załadowania systemu operacyjnego. W celu automatycznego dodania kont Agenta autoryzacji skonfiguruj następujące ustawienia:

- **Podczas szyfrowania automatycznie utwórz konta Agenta autoryzacji dla użytkowników systemu Windows.** Jeśli to pole jest zaznaczone, aplikacja tworzy konta Agenta autoryzacji w oparciu o listę kont użytkowników systemu Windows na komputerze. Domyślnie, Kaspersky Endpoint Security używa wszystkich kont lokalnych i domenowych, z którymi użytkownik logował się do systemu operacyjnego w ciągu ostatnich 30 dni.
- **Automatycznie utwórz konta Agenta autoryzacji dla wszystkich użytkowników tego komputera podczas pierwszego logowania.** Jeśli to pole jest zaznaczone, aplikacja sprawdzi informacje o kontach użytkowników systemu Windows na komputerze przed uruchomieniem Agenta autoryzacji. Jeśli Kaspersky Endpoint Security wykryje konto użytkownika systemu Windows, które nie zawiera konta Agenta autoryzacji, aplikacja utworzy nowe konto do uzyskania dostępu do zaszyfrowanych dysków. Nowe konto Agenta autoryzacji będzie posiadało domyślne ustawienia: tylko logowanie zabezpieczone hasłem oraz zmiana hasła po pierwszej autoryzacji. Dlatego też nie musisz [ręcznie dodawać kont Agenta autoryzacji](#) przy użyciu zadania *Zarządzanie kontami Agenta autoryzacji* dla komputerów z już zaszyfrowanymi dyskami.

Jeśli wyłączyłeś automatyczne tworzenie kont Agenta autoryzacji, możesz [ręcznie dodawać konta Agenta autoryzacji](#) przy użyciu zadania *Zarządzanie kontami*. Możesz także użyć tego zadania do zmiany ustawień kont Agenta autoryzacji, które zostały utworzone automatycznie.

9. Dla wygody użytkownika możesz zapisać nazwę użytkownika w pamięci Agenta autoryzacji, aby przy kolejnym logowaniu do systemu użytkownik musiał wprowadzić tylko hasło. Aby to zrobić, zaznacz pole **Zapisz nazwę użytkownika wprowadzoną w Agencie autoryzacji**.

10. Wybierz jedną z następujących metod szyfrowania:

- Jeśli szyfrowanie chcesz zastosować tylko do tych sektorów dysku twardego, które są zajęte przez pliki, zaznacz pole **Zaszyfruj tylko używaną przestrzeń dyskową**.
Jeśli stosujesz szyfrowanie na dysku, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku. Zapewni to ochronę wszystkich danych, także tych usuniętych, gdyż mogą zawierać informacje, które można odzyskać. Użycie funkcji **Zaszyfruj tylko używaną przestrzeń dyskową** jest zalecane w przypadku nowych dysków, które nie były wcześniej używane.
- Jeśli szyfrowanie chcesz zastosować do całego dysku twardego, odznacz opcję **Zaszyfruj tylko używaną przestrzeń dyskową**.

Jeśli urządzenie zostało wcześniej zaszyfrowane przy użyciu opcji **Szyfruj tylko zajętą przestrzeń dysku (redukuje czas szyfrowania)**, po zastosowaniu zasady w trybie **Zaszyfruj wszystkie dyski twarde**, sektory, które nie są zajęte przez pliki, pozostaną niezaszyfrowane.

11. Jeśli podczas szyfrowania komputera wystąpi problem niekompatybilności sprzętowej, możesz zaznaczyć pole **Obsługa starszych wersji USB (niezalecane)**.

Obsługa starszych wersji USB to funkcja BIOS/UEFI, która umożliwia korzystanie z urządzeń USB (takich jak token zabezpieczający) w trakcie fazy rozruchu komputera przed uruchomieniem systemu operacyjnego (tryb BIOS). Obsługa starszych wersji USB nie wpływa na obsługę urządzeń USB po uruchomieniu systemu operacyjnego.

Jeśli funkcja Obsługa starszych wersji USB jest włączona, Agent autoryzacji w trybie BIOS nie obsługuje pracy z tokenami za pośrednictwem USB. Zalecane jest użycie tej opcji tylko wtedy, gdy istnieje problem kompatybilności sprzętowej i tylko dla tych komputerów, na których wystąpił problem.

12. Zapisz swoje zmiany.

Możesz użyć narzędzia Monitor szyfrowania, aby kontrolować szyfrowanie dysku lub proces deszyfrowania na komputerze użytkownika. Możesz uruchomić narzędzie Monitor szyfrowania z poziomu [okna głównego aplikacji](#).

Jeśli dyski twarde są zaszyfrowane, Agent autoryzacji ładuje się przed uruchomieniem systemu operacyjnego. Użyj Agent autoryzacji do zakończenia procesu autoryzacji, aby uzyskać dostęp do zaszyfrowanych dysków twardych i załadować system operacyjny. Po pomyślnym zakończeniu procedury autoryzacji, system operacyjny zostanie załadowany. Proces autoryzacji jest powtarzany przy każdym ponownym uruchomieniu systemu operacyjnego.

Tworzenie listy dysków twardych wykluczonych z szyfrowania

Listę wykluczeń z szyfrowania można utworzyć tylko dla technologii Kaspersky Disk Encryption.

W celu utworzenia listy dysków twardych wykluczonych z szyfrowania:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
6. Z listy rozwijalnej **Technologia szyfrowania** wybierz opcję **Kaspersky Disk Encryption**.
Wpisy odpowiadające dyskom twardym wykluczonym z szyfrowania pojawią się w tabeli **Nie szyfruj następujących dysków twardych**. Ta tabela jest pusta, jeśli wcześniej nie utworzyłeś listy dysków twardych wykluczonych z szyfrowania.
7. W celu dodania dysków twardych do listy dysków twardych wykluczonych z szyfrowania:
 - a. Kliknij przycisk **Dodaj**.
 - b. W oknie **Dodaj urządzenia z listy Kaspersky Security Center** określ wartości następujących parametrów: **Nazwa**, **Komputer**, **Typ dysku** oraz **Kaspersky Disk Encryption**.
 - c. Kliknij przycisk **Odśwież**.

d. W kolumnie **Nazwa** zaznacz pola obok dysków twardych, które chcesz dodać do listy dysków twardych wykluczonych z szyfrowania.

e. Kliknij **OK**.

Wybrane dyski twarde pojawią się w tabeli **Nie szyfruj następujących dysków twardych**.

8. Jeśli chcesz usunąć dyski twarde z tabeli wykluczeń, zaznacz jeden lub kilka wierszy w tabeli **Nie szyfruj następujących dysków twardych**, a następnie kliknij przycisk **Usuń**.

W przypadku, gdy chcesz wybrać kilka elementów, zaznacz je, trzymając wciśnięty klawisz **CTRL**.

9. Zapisz swoje zmiany.

Eksportowanie i importowanie listy dysków twardych wykluczonych z szyfrowania

Możesz wyeksportować listę wykluczeń szyfrowania dysku twardego do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę wykluczeń tego samego typu. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy wykluczeń lub przeniesienia wykluczeń na inny serwer.

[Eksportowanie i importowanie listy wykluczeń szyfrowania dysku twardego w Konsoli administracyjnej \(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
6. Z listy rozwijalnej **Technologia szyfrowania** wybierz opcję **Kaspersky Disk Encryption**.
Wpisy odpowiadające dyskom twardym wykluczonym z szyfrowania pojawią się w tabeli **Nie szyfruj następujących dysków twardych**.
7. W celu wyeksportowania listy wykluczeń:
 - a. Wybierz wykluczenia, które chcesz wyeksportować. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
Jeśli nie wybrałeś żadnego wykluczenia, Kaspersky Endpoint Security wyeksportuje wszystkie wykluczenia.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML.
8. W celu zaimportowania listy reguł:
 - a. Kliknij przycisk **Importuj**.
 - b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.
 - c. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
9. Zapisz swoje zmiany.

[Eksportowanie i importowanie listy wykluczeń szyfrowania dysku twardego w Web Console](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listę wykluczeń.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
5. Wybierz technologię **Kaspersky Disk Encryption** i kliknij odnośnik, aby skonfigurować ustawienia.
Ustawienia szyfrowania zostaną otwarte.
6. Kliknij odnośnik **Wykluczenia**.
7. W celu wyeksportowania listy reguł:
 - a. Wybierz wykluczenia, które chcesz wyeksportować.
 - b. Kliknij przycisk **Eksportuj**.
 - c. Potwierdź chęć wyeksportowania tylko wybranych wykluczeń lub wyeksportuj całą listę wykluczeń.
 - d. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę wykluczeń, i wybierz folder, w którym chcesz zapisać ten plik.
 - e. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje całą listę wykluczeń do pliku XML.
8. W celu zaimportowania listy reguł:
 - a. Kliknij przycisk **Importuj**.
 - b. W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę wykluczeń.
 - c. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę wykluczeń, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
9. Zapisz swoje zmiany.

Włączanie technologii Single Sign-On (SSO)

Technologia logowania jednokrotnego (SSO) umożliwia automatyczne logowanie do systemu operacyjnego przy użyciu poświadczeń Agenta autoryzacji.

Podczas korzystania z technologii logowania jednokrotnego Agent autoryzacji ignoruje wymagania dotyczące siły hasła określone w Kaspersky Security Center. Możesz ustawić wymagania dotyczące siły hasła w ustawieniach systemu operacyjnego.

Technologia logowania jednokrotnego (SSO) jest niekompatybilna z innymi dostawcami danych uwierzytelniających kont.

Jak włączyć korzystanie z technologii logowania jednokrotnego w Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Szyfrowanie danych** → **Ogólne ustawienia szyfrowania**.
6. W sekcji **Ustawienia hasła** kliknij przycisk **Ustawienia**.
7. W oknie, które zostanie otwarte, na zakładce **Agent autoryzacji** zaznacz pole **Użyj technologii logowania jednokrotnego (SSO)**.
8. Zapisz swoje zmiany.

W rezultacie użytkownik musi przeprowadzić procedurę uwierzytelnienia tylko raz z Agentem. Procedura uwierzytelnienia nie jest wymagana do załadowania systemu operacyjnego. System operacyjny ładuje się automatycznie.

Jak włączyć korzystanie z logowania jednokrotnego w konsoli Web Console?

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz włączyć korzystanie z logowania jednokrotnego.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
5. Wybierz technologię **Kaspersky Disk Encryption** i kliknij odnośnik, aby skonfigurować ustawienia.
Ustawienia szyfrowania zostaną otwarte.
6. W sekcji **Ustawienia hasła** zaznacz pole **Użyj technologii logowania jednokrotnego (SSO)**.
7. Kliknij **OK**.

W rezultacie użytkownik musi przeprowadzić procedurę uwierzytelnienia tylko raz z Agentem. Procedura uwierzytelnienia nie jest wymagana do załadowania systemu operacyjnego. System operacyjny ładuje się automatycznie.

Aby logowanie jednokrotne działało, hasło do konta Windows i hasło do konta Agenta autoryzacji muszą być zgodne. Jeśli hasła się nie zgadzają, użytkownik musi wykonać procedurę uwierzytelnienia dwukrotnie: w interfejsie Agenta autoryzacji i przed załadowaniem systemu operacyjnego. Następnie Kaspersky Endpoint Security zastąpi hasło do konta Agenta autoryzacji hasłem do konta Windows.

Zarządzanie kontami Agenta autoryzacji

Agent autoryzacji jest potrzebny do pracy z dyskami chronionymi za pomocą technologii Kaspersky Disk Encryption (FDE). Przed załadowaniem systemu operacyjnego użytkownik musi zakończyć uwierzytelnianie za pomocą Agenta. Zadanie *Zarządzaj kontami Agenta autoryzacji* służy do konfigurowania ustawień uwierzytelniania użytkownika. Możesz używać zadań lokalnych dla pojedynczych komputerów, a także zadań grupowych dla komputerów z oddzielnych grup administracyjnych lub wybranych komputerów.

Nie można skonfigurować terminarza uruchamiania zadania *Zarządzanie kontami Agenta autoryzacji*. Nie można również przymusowo zatrzymać zadania.

[Jak utworzyć zadanie Zarządzanie kontami Agenta autoryzacji w Konsoli administracyjnej \(MMC\)?](#) 

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zadania**.

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Nowe zadanie**.

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

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (11.7.0)** → **Zarządzanie kontami Agenta autoryzacji**.

Krok 2. Wybieranie polecenia do zarządzania kontem Agenta autoryzacji

Wygeneruj listę poleceń do zarządzania kontem Agenta autoryzacji. Polecenia do zarządzania umożliwiają dodawanie, modyfikowanie i usuwanie kont Agenta autoryzacji (patrz instrukcje poniżej). Tylko użytkownicy posiadający konto Agenta autoryzacji mogą wykonać procedurę uwierzytelnienia, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

Krok 3. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

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

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład `Konta administratora`.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie Kreatora. W razie potrzeby zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

W rezultacie, po zakończeniu zadania, przy następnym uruchomieniu komputera nowy użytkownik może ukończyć procedurę uwierzytelniania, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

[Jak utworzyć zadanie Zarządzanie kontami Agenta autoryzacji w konsoli Web Console?](#) 

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

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

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

2. Na liście rozwijanej **Typ zadania** wybierz **Zarządzanie kontami Agenta autoryzacji**.

3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, Konta administratora.

4. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

Krok 2. Zarządzanie kontami Agenta autoryzacji

Wygeneruj listę poleceń do zarządzania kontem Agenta autoryzacji. Polecenia do zarządzania umożliwiają dodawanie, modyfikowanie i usuwanie kont Agenta autoryzacji (patrz instrukcje poniżej). Tylko użytkownicy posiadający konto Agenta autoryzacji mogą wykonać procedurę uwierzytelnienia, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

Krok 3. Kończenie tworzenia zadania

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

Aby uruchomić zadanie, zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

W rezultacie, po zakończeniu zadania, przy następnym uruchomieniu komputera nowy użytkownik może ukończyć procedurę uwierzytelniania, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

Aby dodać konto Agenta autoryzacji, musisz dodać specjalne polecenie do zadania *Zarządzanie kontami Agenta autoryzacji*. Wygodne jest użycie zadania grupowego, na przykład, w celu dodania konta administratora do wszystkich komputerów.

Kaspersky Endpoint Security umożliwia automatyczne utworzenie kont Agenta autoryzacji przed zaszyfrowaniem dysku. Możesz włączyć automatyczne tworzenie kont Agenta autoryzacji w [ustawieniach zasad Szyfrowania całego dysku](#). Możesz także [użyć technologii jednokrotnego logowania \(SSO\)](#).

[Jak dodać konto Agenta autoryzacji za pomocą Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz właściwości zadania *Zarządzanie kontami Agenta autoryzacji*.
2. W oknie ustawień zadania wybierz sekcję **Opcje**.
3. Kliknij **Dodaj** → **Polecenie dodania konta**.
4. W oknie, które zostanie otwarte, w polu **Konto systemu Windows** określ nazwę konta Microsoft Windows, które zostanie użyte do utworzenia konta Agenta autoryzacji.
5. Jeśli ręcznie wprowadziłeś nazwę konta systemu Windows, kliknij przycisk **Zezwól**, aby zdefiniować identyfikator zabezpieczeń konta (SID).
Jeśli zdecydujesz się nie określać identyfikatora zabezpieczeń (SID) poprzez kliknięcie przycisku **Zezwól**, zostanie on określony w momencie wykonywania zadania na komputerze.

Zdefiniowanie identyfikatora zabezpieczeń konta Windows jest konieczne, aby sprawdzić, czy nazwa konta Windows została wprowadzona poprawnie. Jeśli konto systemu Windows nie istnieje na komputerze lub w zaufanej domenie, zadanie *Zarządzanie kontami Agenta autoryzacji* zakończy się błędem.

6. Zaznacz pole **Zastąp istniejące konto**, jeśli chcesz, żeby istniejące konto, które zostało wcześniej utworzone dla Agenta autoryzacji, zastąpić kontem, które jest aktualnie tworzone.

Ten krok jest dostępny podczas dodawania polecenia tworzenia konta Agenta autoryzacji we właściwościach zadania grupowego do zarządzania kontami Agenta autoryzacji. Ten krok nie jest dostępny podczas dodawania polecenia tworzenia konta Agenta autoryzacji we właściwościach zadania lokalnego *Zarządzanie kontami Agenta autoryzacji*.

7. W polu **Nazwa użytkownika** wpisz nazwę konta Agenta autoryzacji, która ma być wprowadzona podczas procesu autoryzacji, aby uzyskać dostęp do zaszyfrowanych dysków twardych.
8. Zaznacz pole **Zezwól na uwierzytelnianie przy użyciu hasła**, jeśli chcesz, żeby podczas procesu autoryzacji aplikacja pytała użytkownika o wprowadzenie hasła do konta Agenta autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków twardych. Ustaw hasło dla konta Agenta autoryzacji. W razie potrzeby możesz poprosić użytkownika o nowe hasło po pierwszym uwierzytelnieniu.
9. Zaznacz pole **Zezwól na uwierzytelnianie przy użyciu certyfikatu**, jeśli chcesz, żeby podczas procesu autoryzacji aplikacja pytała użytkownika o połączenie tokena lub karty inteligentnej z komputerem w celu uzyskania dostępu do zaszyfrowanych dysków twardych. Wybierz plik certyfikatu do uwierzytelnienia za pomocą karty inteligentnej lub tokena.
10. Jeśli to konieczne, w polu **Opis polecenia** wprowadź szczegółowe informacje dotyczące konta Agenta autoryzacji, których potrzebujesz do zarządzania poleceniem.
11. Wykonaj jedną z poniższych czynności:
 - Zaznacz opcję **Zezwól na autoryzację**, jeśli chcesz, aby aplikacja zezwalała użytkownikowi działającemu pod kontem określonym w poleceniu na dostęp do okna autoryzacji Agenta autoryzacji.
 - Zaznacz opcję **Zablokuj autoryzację**, jeśli chcesz, aby aplikacja blokowała użytkownikowi działającemu pod kontem określonym w poleceniu dostęp do okna autoryzacji Agenta autoryzacji.
12. Zapisz swoje zmiany.

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

Zostanie otwarta lista zadań.

2. Kliknij zadanie **Zarządzanie kontami Agenta autoryzacji** w Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości zadania.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Na liście kont Agenta autoryzacji kliknij przycisk **Dodaj**.

Spowoduje to uruchomienie Kreatora zarządzania kontem Agenta autoryzacji.

5. Wybierz typ polecenia **Dodaj konto**.

6. Wybierz konto użytkownika. Możesz wybrać konto z listy kont domeny lub ręcznie wprowadzić nazwę konta. Kliknij przycisk **Dalej**.

Kaspersky Endpoint Security określa identyfikator zabezpieczeń konta (SID). Jest to konieczne do zweryfikowania konta. Jeśli podałeś nieprawidłową nazwę użytkownika, Kaspersky Endpoint Security zakończy zadanie z błędem.

7. Skonfiguruj ustawienia konta Agenta autoryzacji.

- **Utwórz nowe konto Agenta autoryzacji, aby zastąpić istniejące konto.** Kaspersky Endpoint Security skanuje istniejące konta na komputerze. Jeśli identyfikator zabezpieczeń użytkownika na komputerze i w zadaniu jest zgodny, Kaspersky Endpoint Security zmieni ustawienia konta użytkownika zgodnie z zadaniem.
- **Nazwa użytkownika.** Domyślna nazwa użytkownika konta Agenta autoryzacji odpowiada nazwie domeny użytkownika.
- **Zezwól na uwierzytelnianie przy użyciu hasła.** Ustaw hasło dla konta Agenta autoryzacji. W razie potrzeby możesz poprosić użytkownika o nowe hasło po pierwszym uwierzytelnieniu. W ten sposób każdy użytkownik będzie miał swoje unikatowe hasło. Możesz także ustawić wymagania dotyczące siły hasła dla konta Agenta autoryzacji w zasadzie.
- **Zezwól na uwierzytelnianie przy użyciu certyfikatu.** Wybierz plik certyfikatu do uwierzytelnienia za pomocą karty inteligentnej lub tokena. W ten sposób użytkownik będzie musiał wprowadzić hasło do karty inteligentnej lub tokena.
- **Dostęp konta do zaszyfrowanych danych.** Skonfiguruj dostęp użytkownika do zaszyfrowanego dysku. Możesz, na przykład, tymczasowo wyłączyć uwierzytelnianie użytkownika zamiast usuwać konto Agenta autoryzacji.
- **Komentarz.** W razie potrzeby wprowadź opis konta.

8. Zapisz swoje zmiany.

9. Zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

W rezultacie, po zakończeniu zadania, przy następnym uruchomieniu komputera nowy użytkownik może ukończyć procedurę uwierzytelniania, załadować system operacyjny i uzyskać dostęp do zaszyfrowanego dysku.

Aby zmienić hasło i inne ustawienia konta Agenta autoryzacji, musisz dodać specjalne polecenie do zadania *Zarządzanie kontami Agenta autoryzacji*. Wygodne jest użycie zadania grupowego, na przykład, w celu zastąpienia certyfikatu tokena administratora na wszystkich komputerach.

[Jak zmienić konto Agenta autoryzacji za pomocą Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz właściwości zadania *Zarządzanie kontami Agenta autoryzacji*.
2. W oknie ustawień zadania wybierz sekcję **Opcje**.
3. Kliknij **Dodaj** → **Polecenie edycji konta**.
4. W oknie, które zostanie otwarte, w polu **Konto systemu Windows** określ nazwę konta użytkownika Microsoft Windows, które chcesz zmienić.
5. Jeśli ręcznie wprowadziłeś nazwę konta systemu Windows, kliknij przycisk **Zezwól**, aby zdefiniować identyfikator zabezpieczeń konta (SID).

Jeśli zdecydujesz się nie określać identyfikatora zabezpieczeń (SID) poprzez kliknięcie przycisku **Zezwól**, zostanie on określony w momencie wykonywania zadania na komputerze.

Zdefiniowanie identyfikatora zabezpieczeń konta Windows jest konieczne, aby sprawdzić, czy nazwa konta Windows została wprowadzona poprawnie. Jeśli konto systemu Windows nie istnieje na komputerze lub w zaufanej domenie, zadanie *Zarządzanie kontami Agenta autoryzacji* zakończy się błędem.

6. Zaznacz pole **Zmień nazwę użytkownika** i wprowadź nową nazwę dla konta Agenta autoryzacji, jeśli chcesz, aby Kaspersky Endpoint Security zmienił nazwę użytkownika dla wszystkich kont Agenta autoryzacji, utworzonych w oparciu o konto systemu Microsoft Windows posiadające nazwę określoną w polu **Konto systemu Windows**, na nazwę wpisaną w polu poniżej.
7. Zaznacz pole **Modyfikuj ustawienia uwierzytelniania przy użyciu hasła**, aby możliwe było zmodyfikowanie ustawień autoryzacji opartej o hasło.
8. Zaznacz pole **Zezwól na uwierzytelnianie przy użyciu hasła**, jeśli chcesz, żeby podczas procesu autoryzacji aplikacja pytała użytkownika o wprowadzenie hasła do konta Agenta autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków twardych. Ustaw hasło dla konta Agenta autoryzacji.
9. Zaznacz pole **Edytuj regułę zmiany hasła podczas autoryzacji przy użyciu Agenta autoryzacji**, jeśli chcesz, aby Kaspersky Endpoint Security zmienił wartość ustawienia zmiany hasła dla wszystkich kont Agenta autoryzacji utworzonych w oparciu o konto systemu Microsoft Windows, posiadające nazwę określoną w polu **Konto systemu Windows**, na wartość określoną poniżej.
10. Określ wartość ustawienia zmiany hasła po autoryzacji w Agencie autoryzacji.
11. Zaznacz pole **Modyfikuj ustawienia uwierzytelniania przy użyciu certyfikatu**, aby możliwe było zmodyfikowanie ustawień autoryzacji opartej o certyfikat elektroniczny tokena lub karty inteligentnej.
12. Zaznacz pole **Zezwól na uwierzytelnianie przy użyciu certyfikatu**, jeśli chcesz, żeby podczas procesu autoryzacji aplikacja pytała użytkownika o wprowadzenie hasła do tokena lub karty inteligentnej podłączonej do komputera w celu uzyskania dostępu do zaszyfrowanych dysków twardych. Wybierz plik certyfikatu do uwierzytelnienia za pomocą karty inteligentnej lub tokena.
13. Zaznacz pole **Edytuj opis polecenia** i zmodyfikuj opis polecenia, jeśli chcesz, aby Kaspersky Endpoint Security zmienił opis polecenia dla wszystkich kont Agenta autoryzacji, utworzonych w oparciu o konto systemu Microsoft Windows posiadające nazwę określoną w polu **Konto systemu Windows**.
14. Zaznacz pole **Edytuj regułę dostępu do autoryzacji przy użyciu Agenta Autoryzacji**, jeśli chcesz, aby Kaspersky Endpoint Security zmienił regułę dostępu użytkownika do okna autoryzacji w Agencie autoryzacji na wartość określoną poniżej dla wszystkich kont Agenta autoryzacji, utworzonych w oparciu o konto systemu Microsoft Windows posiadające nazwę określoną w polu **Konto systemu Windows**.

15. Określ regułę dostępu do okna autoryzacji w Agencie autoryzacji.

16. Zapisz swoje zmiany.

[Jak zmienić konto Agenta autoryzacji za pomocą konsoli Web Console?](#) 

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

Zostanie otwarta lista zadań.

2. Kliknij zadanie **Zarządzanie kontami Agenta autoryzacji** w Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości zadania.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Na liście kont Agenta autoryzacji kliknij przycisk **Dodaj**.

Spowoduje to uruchomienie Kreatora zarządzania kontem Agenta autoryzacji.

5. Wybierz typ polecenia **Edytuj konto**.

6. Wybierz konto użytkownika. Możesz wybrać konto z listy kont domeny lub ręcznie wprowadzić nazwę konta. Kliknij przycisk **Dalej**.

Kaspersky Endpoint Security określa identyfikator zabezpieczeń konta (SID). Jest to konieczne do zweryfikowania konta. Jeśli podałeś nieprawidłową nazwę użytkownika, Kaspersky Endpoint Security zakończy zadanie z błędem.

7. Zaznacz pola wyboru obok ustawień, które chcesz edytować.

8. Skonfiguruj ustawienia konta Agenta autoryzacji.

- **Utwórz nowe konto Agenta autoryzacji, aby zastąpić istniejące konto.** Kaspersky Endpoint Security skanuje istniejące konta na komputerze. Jeśli identyfikator zabezpieczeń użytkownika na komputerze i w zadaniu jest zgodny, Kaspersky Endpoint Security zmieni ustawienia konta użytkownika zgodnie z zadaniem.
- **Nazwa użytkownika.** Domyślna nazwa użytkownika konta Agenta autoryzacji odpowiada nazwie domeny użytkownika.
- **Zezwól na uwierzytelnianie przy użyciu hasła.** Ustaw hasło dla konta Agenta autoryzacji. W razie potrzeby możesz poprosić użytkownika o nowe hasło po pierwszym uwierzytelnieniu. W ten sposób każdy użytkownik będzie miał swoje unikatowe hasło. Możesz także ustawić wymagania dotyczące siły hasła dla konta Agenta autoryzacji w zasadzie.
- **Zezwól na uwierzytelnianie przy użyciu certyfikatu.** Wybierz plik certyfikatu do uwierzytelnienia za pomocą karty inteligentnej lub tokena. W ten sposób użytkownik będzie musiał wprowadzić hasło do karty inteligentnej lub tokena.
- **Dostęp konta do zaszyfrowanych danych.** Skonfiguruj dostęp użytkownika do zaszyfrowanego dysku. Możesz, na przykład, tymczasowo wyłączyć uwierzytelnianie użytkownika zamiast usuwać konto Agenta autoryzacji.
- **Komentarz.** W razie potrzeby wprowadź opis konta.

9. Zapisz swoje zmiany.

10. Zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

Aby usunąć konto Agenta autoryzacji, musisz dodać specjalne polecenie do zadania *Zarządzanie kontami Agenta autoryzacji*. Wygodnie jest skorzystać z zadania grupowego, na przykład, aby usunąć konto zwolnionego pracownika.

Jak usunąć konto Agenta autoryzacji za pomocą Konsoli administracyjnej.(MMC)?

1. Otwórz właściwości zadania *Zarządzanie kontami Agenta autoryzacji*.
2. W oknie ustawień zadania wybierz sekcję **Opcje**.
3. Kliknij opcję **Dodaj** → **Polecenie usunięcia konta**.
4. W otwartym oknie, w polu **Konto systemu Windows** określ nazwę konta użytkownika systemu Windows, w oparciu o które zostało utworzone konto Agenta autoryzacji, które chcesz usunąć.
5. Jeśli ręcznie wprowadziłeś nazwę konta systemu Windows, kliknij przycisk **Zezwól**, aby zdefiniować identyfikator zabezpieczeń konta (SID).

Jeśli zdecydujesz się nie określać identyfikatora zabezpieczeń (SID) poprzez kliknięcie przycisku **Zezwól**, zostanie on określony w momencie wykonywania zadania na komputerze.

Zdefiniowanie identyfikatora zabezpieczeń konta Windows jest konieczne, aby sprawdzić, czy nazwa konta Windows została wprowadzona poprawnie. Jeśli konto systemu Windows nie istnieje na komputerze lub w zaufanej domenie, zadanie *Zarządzanie kontami Agenta autoryzacji* zakończy się błędem.

6. Zapisz swoje zmiany.

Jak usunąć konto Agenta autoryzacji za pomocą konsoli Web Console?

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Kliknij zadanie **Zarządzanie kontami Agenta autoryzacji** w Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości zadania.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Na liście kont Agenta autoryzacji kliknij przycisk **Dodaj**.
Spowoduje to uruchomienie Kreatora zarządzania kontem Agenta autoryzacji.
5. Wybierz typ polecenia **Usuń konto**.
6. Wybierz konto użytkownika. Możesz wybrać konto z listy kont domeny lub ręcznie wprowadzić nazwę konta.
7. Zapisz swoje zmiany.
8. Zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

W rezultacie, po zakończeniu zadania, przy następnym uruchomieniu komputera użytkownik nie będzie mógł ukończyć procedury uwierzytelniania i załadować systemu operacyjnego. Kaspersky Endpoint Security odmówi dostępu do zaszyfrowanych danych.

Aby wyświetlić listę użytkowników, którzy mogą ukończyć uwierzytelnianie za pomocą Agenta i załadować system operacyjny, musisz przejść do właściwości zarządzanego komputera.

Jak wyświetlić listę kont Agenta autoryzacji za pomocą Konsoli administracyjnej (MMC)?

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Kliknij dwukrotnie komputer, aby otworzyć okno właściwości komputera.
5. W oknie właściwości komputera wybierz sekcję **Zadania**.
Zostanie otwarta lista zadań lokalnych.
6. Wybierz zadanie **Zarządzanie kontami Agenta autoryzacji**.
7. W oknie ustawień zadania wybierz sekcję **Opcje**.

Dzięki temu będziesz mógł uzyskać dostęp do listy kont Agenta autoryzacji na tym komputerze. Tylko użytkownicy z listy mogą zakończyć uwierzytelnianie za pomocą Agenta i załadować system operacyjny.

Jak wyświetlić listę kont Agenta autoryzacji za pomocą konsoli Web Console?

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Kliknij nazwę komputera, na którym chcesz wyświetlić listę kont Agenta autoryzacji.
Spowoduje to otwarcie właściwości komputera.
3. W oknie właściwości komputera wybierz sekcję **Zadania**.
Zostanie otwarta lista zadań lokalnych.
4. Wybierz zadanie **Zarządzanie kontami Agenta autoryzacji**.
5. We właściwościach zadania wybierz zakładkę **Ustawienia aplikacji**.

Dzięki temu będziesz mógł uzyskać dostęp do listy kont Agenta autoryzacji na tym komputerze. Tylko użytkownicy z listy mogą zakończyć uwierzytelnianie za pomocą Agenta i załadować system operacyjny.

Używanie tokenów i kart inteligentnych z Agentem autoryzacji

Token lub karta inteligentna mogą zostać użyte do autoryzacji podczas dostępu do zaszyfrowanych dysków twardych. Aby to zrobić, musisz dodać plik certyfikatu elektronicznego tokena lub karty inteligentnej do zadania *Zarządzanie kontami Agenta autoryzacji*.

Użycie tokena lub karty inteligentnej jest możliwe tylko wtedy, gdy dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES256. Jeśli dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES56, dodanie pliku certyfikatu elektronicznego do polecenia zostanie odrzucone.

Kaspersky Endpoint Security obsługuje następujące tokeny, czytniki kart inteligentnych oraz karty inteligentne:

- SafeNet eToken PRO 64K (4.2b);
- SafeNet eToken PRO 72K Java;
- SafeNet eToken 4100-72K Java;
- SafeNet eToken 5100;
- SafeNet eToken 5105;
- SafeNet eToken 7300;
- EMC RSA SID 800;
- Gemalto IDPrime.NET 510;
- Gemalto IDPrime.NET 511;
- Rutoken ECP;
- Rutoken ECP Flash;
- Athena IDProtect Laser;
- SafeNet eToken PRO 72K Java;
- Aladdin-RD JaCarta PKI.

Aby dodać plik certyfikatu elektronicznego tokena lub karty inteligentnej do polecenia tworzenia konta Agenta autoryzacji, w pierwszej kolejności zapisz plik, korzystając z oprogramowania firmy trzeciej do zarządzania certyfikatami.

Certyfikat tokena lub karty inteligentnej musi posiadać następujące parametry:

- Certyfikat musi być zgodny ze standardem X.509, a plik certyfikatu musi być kodowany przy użyciu algorytmu DER.
- Certyfikat zawiera klucz RSA o długości minimum 1024 bitów.

Jeśli certyfikat elektroniczny tokena lub karty inteligentnej nie spełnia tych wymagań, nie można załadować pliku certyfikatu do polecenia utworzenia konta Agenta autoryzacji.

Parametr KeyUsage certyfikatu musi posiadać wartość keyEncipherment lub dataEncipherment. Parametr KeyUsage określa cel certyfikatu. Jeśli parametr ma inną wartość, Kaspersky Security Center pobierze plik certyfikatu, ale wyświetli ostrzeżenie.

Jeśli użytkownik zgubił token lub kartę inteligentną, administrator musi dodać plik certyfikatu elektronicznego tokena lub karty inteligentnej do polecenia tworzenia konta Agenta autoryzacji. Następnie użytkownik musi przejść procedurę [przywracania dostępu do zaszyfrowanych urządzeń lub przywracania danych na zaszyfrowanych urządzeniach](#).

Deszyfrowanie dysków twardych

Dyski twarde można odszyfrować nawet wtedy, gdy nie ma aktywnej licencji zezwalającej na szyfrowanie danych.

W celu odszyfrowania dysków twardych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
6. Z listy rozwijalnej **Technologia szyfrowania** wybierz technologię, za pomocą której zostały zaszyfrowane dyski twarde.
7. Wykonaj jedną z poniższych czynności:
 - Z listy rozwijalnej **Tryb szyfrowania** wybierz opcję **Odszyfruj wszystkie dyski twarde**, jeśli chcesz odszyfrować wszystkie zaszyfrowane dyski twarde.
 - Dodaj zaszyfrowane dyski twarde, które chcesz odszyfrować, do tabeli **Nie szyfruj następujących dysków twardych**.

Ta opcja jest dostępna tylko dla technologii Kaspersky Disk Encryption.

8. Zapisz swoje zmiany.

Możesz użyć narzędzia Monitor szyfrowania, aby kontrolować szyfrowanie dysku lub proces deszyfrowania na komputerze użytkownika. Możesz uruchomić narzędzie Monitor szyfrowania z poziomu [okna głównego aplikacji](#).

Jeśli podczas deszyfrowania dysków twardych, zaszyfrowanych za pomocą technologii Kaspersky Disk Encryption, użytkownik zamknie lub uruchomi ponownie komputer, Agent autoryzacji załaduje się przed kolejnym uruchomieniem systemu operacyjnego. Kaspersky Endpoint Security wznawia deszyfrowanie dysku twardego po pomyślnej autoryzacji w Agencji autoryzacji i uruchomieniu systemu operacyjnego.

Jeśli podczas deszyfrowania dysków twardych, zaszyfrowanych za pomocą technologii Kaspersky Disk Encryption, system operacyjny przełączy się w tryb hibernacji, Agent autoryzacji załaduje się po wyjściu systemu operacyjnego z trybu hibernacji. Kaspersky Endpoint Security wznawia deszyfrowanie dysku twardego po pomyślnej autoryzacji w Agencji autoryzacji i uruchomieniu systemu operacyjnego. Po odszyfrowaniu dysku twardego, tryb hibernacji jest niedostępny, aż do pierwszego ponownego uruchomienia systemu operacyjnego.

Jeśli podczas deszyfrowania dysku twardego system operacyjny przejdzie w tryb uśpienia, Kaspersky Endpoint Security wznowi deszyfrowanie dysku twardego po wyjściu systemu operacyjnego z trybu uśpienia, bez wczytywania Agenta autoryzacji.

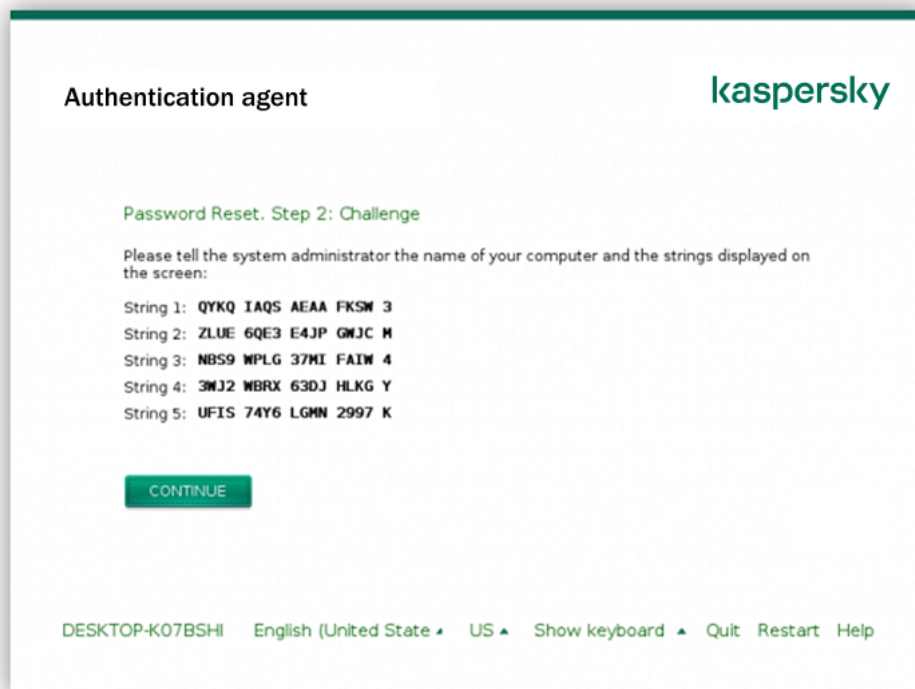
Przywracanie dostępu do dysku chronionego przez technologię Kaspersky Disk Encryption

Jeśli użytkownik zapomniał hasła dostępu do dysku twardego chronionego przez technologię Kaspersky Disk Encryption, musisz rozpocząć procedurę odzyskiwania (Żądanie-Odpowiedź).

Przywracanie dostępu do systemowego dysku twardego

Przywrócenie dostępu do systemowego dysku twardego chronionego technologią Kaspersky Disk Encryption składa się z następujących kroków:

1. Użytkownik zgłasza blokady administratorowi (patrz rysunek poniżej).
2. Administrator wprowadza sekcje zgłoszeń do Kaspersky Security Center, odbiera sekcje odpowiedzi i zgłasza sekcje odpowiedzi użytkownikowi.
3. Użytkownik wprowadza sekcje odpowiedzi w interfejsie Agenta autoryzacji i uzyskuje dostęp do dysku twardego.



Przywracanie dostępu do systemowego dysku twardego chronionego przez technologię Kaspersky Disk Encryption

Aby rozpocząć procedurę odzyskiwania, użytkownik musi kliknąć przycisk **Nie pamiętam hasła** w interfejsie Agenta autoryzacji.

[Jak uzyskać sekcje odpowiedzi dla systemowego dysku twardego chronionego przez technologię Kaspersky Disk Encryption w Konsoli administracyjnej \(MMC\)](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Na zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy.
5. Z menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.
6. W otwartym oknie wybierz zakładkę **Agent autoryzacji**.
7. W sekcji **Używany algorytm szyfrujący** wybierz algorytm szyfrowania: **AES56** lub **AES256**.

Algorytm szyfrowania danych zależy od biblioteki szyfrowania AES zawartej w pakiecie dystrybucyjnym: *Silne szyfrowanie (AES256)* lub *Uprozczone szyfrowanie (AES56)*. Biblioteka szyfrowania AES jest instalowana wraz z aplikacją.

8. Z listy rozwijalnej **Konto** wybierz nazwę konta Agenta autoryzacji użytkownika, który prosi o przywrócenie dostępu do dysku.
9. Z listy rozwijalnej **Dysk twardy** wybierz zaszyfrowany dysk twardy, dla którego chcesz przywrócić dostęp.
10. W sekcji **Żądanie użytkownika** wprowadź sekcje ze zgłoszeniami użytkownika.

W rezultacie, zawartość sekcji z odpowiedziami na żądanie użytkownika dotyczące przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji będzie wyświetlana w polu **Klucz dostępu**. Prześlij zawartość sekcji odpowiedzi do użytkownika.

[Jak uzyskać sekcje odpowiedzi dla systemowego dysku twardego chronionego przez technologię Kaspersky Disk Encryption w konsoli Web Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Zaznacz pole wyboru obok nazwy komputera, do dysku którego chcesz przywrócić dostęp.
3. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.
4. W otwartym oknie wybierz sekcję **Agent autoryzacji**.
5. Z listy rozwijalnej **Konto** wybierz nazwę konta Agenta autoryzacji utworzonego dla użytkownika, który prosi o przywrócenie nazwy konta i hasła dla Agenta autoryzacji.
6. Wprowadź sekcje żądań przesłane przez użytkownika.

Zawartość sekcji z odpowiedziami na żądanie użytkownika dotyczące przywrócenia nazwy użytkownika i hasła dla konta Agenta autoryzacji będzie wyświetlana w dolnej części okna. Prześlij zawartość sekcji odpowiedzi do użytkownika.

Po zakończeniu procedury odzyskiwania Agent autoryzacji poprosi użytkownika o zmianę hasła.

Przywracanie dostępu do niesystemowego dysku twardego

Przywrócenie dostępu do niesystemowego dysku twardego chronionego technologią Kaspersky Disk Encryption składa się z następujących kroków:

1. Użytkownik wyśle plik zawierający żądanie dostępu do administratora.
2. Administrator dodaje plik żądania dostępu do Kaspersky Security Center, tworzy plik klucza dostępu i wysyła ten plik do użytkownika.
3. Użytkownik dodaje plik klucza dostępu do Kaspersky Endpoint Security i uzyskuje dostęp do dysku twardego.

Aby rozpocząć procedurę odzyskiwania, użytkownik musi spróbować uzyskać dostęp do dysku twardego. W rezultacie Kaspersky Endpoint Security utworzy plik dostępu do żądania (plik z rozszerzeniem KESDC), który użytkownik musi wysłać administratorowi, na przykład, za pośrednictwem poczty elektronicznej.

[Jak uzyskać plik klucza dostępu do zaszyfrowanego niesystemowego dysku twardego w Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Na zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy.
5. Z menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.
6. W otwartym oknie wybierz zakładkę **Szyfrowanie danych**.
7. Na zakładce **Szyfrowanie danych** kliknij przycisk **Przełóżaj**.
8. W oknie wyboru pliku dostępu do żądania określ ścieżkę do pliku otrzymanego od użytkownika.

Zobaczysz informacje o żądaniu użytkownika. Kaspersky Security Center wygeneruje plik klucza. Wyślij do użytkownika wygenerowany plik klucza dostępu do zaszyfrowanych danych. Lub zapisz plik dostępu i użyj dowolnej dostępnej metody, aby przenieść plik.

[Jak uzyskać zaszyfrowany niesystemowy plik klucza dostępu do dysku twardego w konsoli Web Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Zaznacz pole wyboru obok nazwy komputera, do którego danych chcesz przywrócić dostęp.
3. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.
4. Wybierz sekcję **Szyfrowanie danych**.
5. Kliknij przycisk **Wybierz plik** i wybierz plik żądania dostępu otrzymany od użytkownika (plik z rozszerzeniem KESDC).
Konsola Web Console wyświetli informacje o żądaniu. Obejmuje to nazwę komputera, na którym użytkownik żąda dostępu do pliku.
6. Kliknij przycisk **Zapisz klucz** i wybierz folder, aby zapisać plik klucza dostępu do zaszyfrowanych danych (plik z rozszerzeniem KESDR).

W rezultacie będziesz mógł uzyskać klucz dostępu do zaszyfrowanych danych, który będziesz musiał przekazać użytkownikowi.

Aktualizowanie systemu operacyjnego

Istnieje szereg specjalnych uwag dotyczących aktualizacji systemu operacyjnego komputera chronionego przez Szyfrowanie całego dysku (FDE). Zaktualizuj system operacyjny w następujący sposób: najpierw zaktualizuj system operacyjny na jednym komputerze, następnie zaktualizuj system operacyjny na małej części komputerów, a następnie zaktualizuj system operacyjny na wszystkich komputerach w sieci.

Jeśli korzystasz z technologii Kaspersky Disk Encryption, Agent autoryzacji jest ładowany przed uruchomieniem systemu operacyjnego. Korzystając z Agenta autoryzacji, użytkownik może zalogować się do systemu i uzyskać dostęp do zaszyfrowanych dysków. Następnie system operacyjny zaczyna się ładować.

Jeśli rozpoczniesz aktualizację systemu operacyjnego na komputerze chronionym przy użyciu technologii Kaspersky Disk Encryption, Kreator aktualizacji systemu operacyjnego usunie Agenta autoryzacji. W rezultacie komputer może zostać zablokowany, ponieważ moduł ładujący system operacyjny nie będzie mógł uzyskać dostępu do zaszyfrowanego dysku.

Szczegółowe informacje na temat bezpiecznej aktualizacji systemu operacyjnego można znaleźć w [Bazie wiedzy pomocy technicznej](#).

Automatyczna aktualizacja systemu operacyjnego jest dostępna pod następującymi warunkami:

1. System operacyjny jest aktualizowany przez WSUS (Windows Server Update Services).
2. System Windows 10 w wersji 1607 (RS1) lub nowszy jest zainstalowany na komputerze.
3. Kaspersky Endpoint Security w wersji 11.2 lub nowszej jest zainstalowany na komputerze.

Jeśli wszystkie warunki są spełnione, możesz zaktualizować system operacyjny w zwykły sposób.

Jeśli korzystasz z technologii Kaspersky Disk Encryption (FDE) i Kaspersky Endpoint Security for Windows w wersji 11.0 lub 11.1 jest zainstalowana na komputerze, nie potrzebujesz odszyfrować dysków twardej do przeprowadzenia aktualizacji Windows 10.

W celu zaktualizowania systemu operacyjnego należy wykonać następujące czynności:

1. Przed zaktualizowaniem systemu skopiuj sterowniki o nazwie cm_km.inf, cm_km.sys, klfde.cat, klfde.inf, klfde.sys, klfdefsf.cat, klfdefsf.inf i klfdefsf.sys do folderu lokalnego. Na przykład: C:\fde_drivers.
2. Uruchom instalację aktualizacji systemu z przełącznikiem `/ReflectDrivers` i określ folder zawierający zapisane dyski:
`setup.exe /ReflectDrivers C:\fde_drivers`

Jeśli używasz technologii szyfrowania BitLocker, nie musisz odszyfrowywać dysków twardych, aby zaktualizować system Windows 10. Więcej informacji na temat działania BitLocker znajdziesz na [stronie internetowej firmy Microsoft](#).

Eliminowanie błędów aktualizacji funkcjonalności szyfrowania

Szyfrowanie całego dysku jest aktualizowane, gdy poprzednia wersja aplikacji zostanie zaktualizowana do Kaspersky Endpoint Security for Windows 11.7.0.

Podczas uruchamiania aktualizacji funkcjonalności Szyfrowanie całego dysku mogą wystąpić następujące błędy:

- Brak możliwości zainicjowania aktualizacji.
- Urządzenie nie jest kompatybilne z Agentem autoryzacji.

W celu wyeliminowania błędów, które wystąpiły podczas uruchamiania procesu aktualizacji funkcjonalności Szyfrowanie całego dysku w nowej wersji aplikacji:

1. [Odszyfruj dyski twarde.](#)
2. Ponownie [zaszyfruj dyski twarde.](#)

Podczas aktualizacji funkcjonalności Szyfrowanie całego dysku mogą wystąpić następujące błędy:

- Brak możliwości zakończenia aktualizacji.
- Wycofanie aktualizacji Szyfrowania całego dysku zakończyło się błędem.

W celu wyeliminowania błędów, które wystąpiły podczas procesu aktualizacji funkcjonalności Szyfrowanie całego dysku:

[Przywróć dostęp do zaszyfrowanych urządzeń przy użyciu Narzędzia przywracania zaszyfrowanego urządzenia.](#)

Wybieranie poziomu śledzenia Agentu autoryzacji

Aplikacja zapisuje w pliku śledzenia informacje serwisowe o działaniu Agentu autoryzacji oraz informacje o działaniach użytkownika dotyczących Agentu autoryzacji.

W celu wybrania poziomu śledzenia Agentu autoryzacji:

1. Jak tylko uruchomi się komputer z zaszyfrowanymi dyskami twardymi, wciśnij klawisz **F3**, aby wywołać okno konfiguracji ustawień Agentu autoryzacji.
2. W oknie ustawień Agentu autoryzacji wybierz poziom śledzenia:

- **Wyłącz rejestrowanie debugowania (domyślny).** Jeśli ta opcja jest zaznaczona, aplikacja nie rejestruje informacji o zdarzeniach Agenta autoryzacji w pliku śledzenia.
- **Włącz rejestrowanie debugowania.** Jeśli ta opcja jest zaznaczona, aplikacja rejestruje w pliku śledzenia informacje dotyczące działania Agenta autoryzacji oraz działań użytkownika wykonywanych na Agencie autoryzacji.
- **Włącz rejestrowanie w trybie informacji pełnej.** Jeśli ta opcja jest zaznaczona, aplikacja rejestruje w pliku śledzenia szczegółowe informacje dotyczące działania Agenta autoryzacji oraz działań użytkownika wykonywanych na Agencie autoryzacji.

Poziom szczegółowości wpisów w tej opcji jest wyższy niż w opcji **Włącz rejestrowanie debugowania**. Wysoki poziom szczegółowości wpisów może spowalniać uruchamianie Agenta autoryzacji i systemu operacyjnego.

- **Włącz rejestrowanie debugowania i wybierz port szeregowy.** Jeśli ta opcja jest zaznaczona, aplikacja rejestruje w pliku śledzenia informacje dotyczące działania Agenta autoryzacji oraz działań użytkownika wykonywanych na Agencie autoryzacji i przesyła je poprzez port COM.
Jeśli komputer z zaszyfrowanymi dyskami twardymi jest podłączony do innego komputera poprzez port COM, zdarzenia Agenta autoryzacji mogą zostać sprawdzone z tego innego komputera.
- **Włącz rejestrowanie debugowania w trybie informacji pełnej i wybierz port szeregowy.** Jeśli ta opcja jest zaznaczona, aplikacja rejestruje w pliku śledzenia szczegółowe informacje dotyczące działania Agenta autoryzacji oraz działań użytkownika wykonywanych na Agencie autoryzacji i przesyła je poprzez port COM.

Poziom szczegółowości wpisów w tej opcji jest wyższy niż w opcji **Włącz rejestrowanie debugowania i wybierz port szeregowy**. Wysoki poziom szczegółowości wpisów może spowalniać uruchamianie Agenta autoryzacji i systemu operacyjnego.

Dane są zapisywane w pliku śledzenia Agenta autoryzacji, jeśli na komputerze lub podczas szyfrowania całego dysku znajdują się zaszyfrowane dyski twarde.

W przeciwieństwie do innych plików śledzenia aplikacji, plik śledzenia Agenta autoryzacji nie jest wysyłany na serwer Kaspersky. Jeśli jest to konieczne, możesz ręcznie wysłać plik śledzenia Agenta autoryzacji do Kaspersky w celu przeprowadzenia jego analizy.

Modyfikowanie komunikatów pomocy Agenta Autoryzacji

Przed zmodyfikowaniem komunikatów pomocy Agenta Autoryzacji należy przejrzeć listę znaków obsługiwanych w środowisku wykonawczym przed uruchomieniem systemu (patrz poniżej).

W celu zmodyfikowania komunikaty pomocy Agenta Autoryzacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

5. W oknie zasady wybierz **Szyfrowanie danych** → **Ogólne ustawienia szyfrowania**.

6. W sekcji **Szablony** kliknij przycisk **Pomoc**.

Zostanie otwarte okno **Komunikaty pomocy Agenta Autoryzacji**.

7. Wykonaj następujące czynności:

- Wybierz zakładkę **Autoryzacja**, aby zmodyfikować treść wiadomości pomocy wyświetlanej w oknie Agenta autoryzacji podczas wprowadzania danych uwierzytelniających konta.
- Wybierz zakładkę **Zmiana hasła**, aby zmodyfikować treść wiadomości pomocy wyświetlanej w oknie Agenta autoryzacji, gdy zmieniane jest hasło do konta Agenta autoryzacji.
- Wybierz zakładkę **Przywracanie hasła**, aby zmodyfikować treść wiadomości pomocy wyświetlanej w oknie Agenta autoryzacji, gdy odzyskiwane jest hasło do konta Agenta autoryzacji.

8. Zmodyfikuj treść pomocy.

Jeśli chcesz przywrócić oryginalny tekst, kliknij przycisk **Domyślny**.

Wprowadzana treść pomocy powinna zawierać 16 linijek lub mniej. Maksymalna długość wiersza to 64 znaki.

9. Zapisz swoje zmiany.

Ograniczona obsługa znaków w wiadomościach pomocy Agenta autoryzacji

W środowisku wykonawczym przed uruchomieniem systemu obsługiwane są następujące znaki Unicode:

- Alfabet łaciński podstawowy (0000 - 007F)
- Dodatkowe znaki alfabetu łacińskiego Latin-1 (0080 - 00FF)
- Łaciński rozszerzony Latin-A (0100 - 017F)
- Łaciński rozszerzony Latin-B (0180 - 024F)
- Oddzielone litery modyfikujące (02B0 - 02FF)
- Składające znaki diakrytyczne (0300 - 036F)
- Alfabet grecki i alfabet koptyjski (0370 - 03FF)
- Cyrylica (0400 - 04FF)
- Hebrajski (0590 - 05FF)
- Arabski (0600 - 06FF)
- Łaciński rozszerzony dodatkowy (1E00 - 1EFF)
- Znaki interpunkcyjne (2000 - 206F)
- Symbole walut (20A0 - 20CF)

- Symbole literopodobne (2100 - 214F)
- Figury geometryczne (25A0 - 25FF)
- Arabskie formy prezentacyjne B (FE70 - FEFF)

Znaki, które nie zostały wymienione na liście, nie są obsługiwane w środowisku wykonawczym przed uruchomieniem systemu. Nie jest zalecane używanie tych znaków w wiadomościach pomocy Agenta autoryzacji.

Usuwanie obiektów i danych pozostałych po testowym działaniu Agenta autoryzacji

Podczas dezinstalacji aplikacji, jeśli Kaspersky Endpoint Security wykryje obiekty i dane, które pozostały na dysku twardym po działaniu Agenta autoryzacji, dezinstalacja aplikacji zostanie przerwana i nie będzie możliwa, dopóki te obiekty nie zostaną usunięte.

Obiekty i dane mogą pozostać na dysku twardym po testowym działaniu Agenta autoryzacji tylko w wyjątkowych przypadkach. Na przykład wtedy, gdy komputer nie został uruchomiony ponownie po zastosowaniu profilu Kaspersky Security Center z ustawieniami szyfrowania lub gdy nie powiodło się uruchomienie aplikacji po testowym działaniu Agenta autoryzacji.

Obiekty i dane pozostające na dysku twardym po testowym działaniu Agenta autoryzacji można usunąć na następujące sposoby:

- Przy pomocy profilu Kaspersky Security Center.
- [Przy użyciu Narzędzia przywracania zaszyfrowanego urządzenia.](#)

W celu użycia profilu Kaspersky Security Center do usunięcia obiektów i danych, które pozostały po testowym działaniu Agenta autoryzacji:

1. Zastosuj na komputerze profil Kaspersky Security Center z ustawieniami skonfigurowanymi do [deszyfracji](#) wszystkich dysków twardych komputera.
2. Uruchom Kaspersky Endpoint Security.

W celu usunięcia informacji o niekompatybilności aplikacji z Agentem autoryzacji:

w wierszu polecenia wprowadź `avp pbatestreset`.

Zarządzanie BitLocker

BitLocker to technologia szyfrowania wbudowana w systemy operacyjne Windows. Kaspersky Endpoint Security pozwala kontrolować i zarządzać BitLocker za pomocą Kaspersky Security Center. BitLocker szyfruje woluminy logiczne. Funkcja BitLocker nie może być używana do szyfrowania dysków wymiennych. Więcej informacji na temat BitLocker można znaleźć w [dokumentacji firmy Microsoft](#).

Funkcja BitLocker zapewnia bezpieczne przechowywanie kluczy dostępu za pomocą zaufanego modułu platformy. *Moduł TPM (Trusted Platform Module)* to mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład, do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej. Korzystanie z modułu TPM jest najbezpieczniejszym sposobem przechowywania kluczy dostępu funkcji BitLocker, ponieważ moduł TPM zapewnia weryfikację integralności systemu przed uruchomieniem. Nadal możesz szyfrować dyski na komputerze bez modułu TPM. W takim przypadku klucz dostępu zostanie zaszyfrowany przy użyciu hasła. Funkcja BitLocker używa następujących metod uwierzytelniania:

- TPM.
- TPM i PIN.
- Hasło.

Po zaszyfrowaniu dysku funkcja BitLocker tworzy klucz główny. Kaspersky Endpoint Security wysyła klucz główny do Kaspersky Security Center, abyś mógł [przywrócić dostęp do dysku](#), na przykład, jeśli użytkownik zapomniał hasła.

Jeśli użytkownik zaszyfruje dysk przy użyciu funkcji BitLocker, Kaspersky Endpoint Security wyśle [informacje o szyfrowaniu dysku do Kaspersky Security Center](#). Jednak Kaspersky Endpoint Security nie wyśle klucza głównego do Kaspersky Security Center, więc przywrócenie dostępu do dysku za pomocą Kaspersky Security Center będzie niemożliwe. Aby funkcja BitLocker działała poprawnie z Kaspersky Security Center, [odszyfruj dysk](#) i [ponownie zaszyfruj dysk](#) przy użyciu zasady. Możesz odszyfrować dysk lokalnie lub za pomocą zasady.

Po zaszyfrowaniu systemowego dysku twardego użytkownik musi przejść uwierzytelnianie funkcją BitLocker, aby uruchomić system operacyjny. Po procedurze uwierzytelniania funkcja BitLocker pozwoli użytkownikom zalogować się. Funkcja BitLocker nie obsługuje technologii pojedynczego logowania (SSO).

Jeśli używasz zasad grupy Windows, wyłącz zarządzanie funkcją BitLocker w ustawieniach zasad. Ustawienia zasad Windows mogą kolidować z ustawieniami zasad Kaspersky Endpoint Security. Podczas szyfrowania dysku mogą wystąpić błędy.

Uruchamianie Szyfrowania dysków funkcją BitLocker

Przed uruchomieniem szyfrowania całego dysku zalecane jest upewnienie się, że komputer nie jest zainfekowany. W tym celu uruchom zadanie Pełne skanowanie lub Skanowanie obszarów krytycznych. Wykonanie szyfrowania całego dysku na komputerze, który jest zainfekowany rootkitem, może spowodować, że komputer przestanie działać.

Aby użyć Szyfrowania dysków funkcją BitLocker na komputerach z systemem operacyjnym Windows dla serwerów, może być wymagana instalacja komponentu Szyfrowanie dysków funkcją BitLocker. Zainstaluj komponent za pomocą narzędzi systemu operacyjnego (Kreator dodawania ról i komponentów). Więcej informacji o instalowaniu szyfrowania dysków funkcją BitLocker można znaleźć w [dokumentacji firmy Microsoft](#).

[Jak uruchomić szyfrowanie dysków funkcją BitLocker za pomocą Konsoli administracyjnej.\(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
6. Z listy rozwijalnej **Technologia szyfrowania** wybierz opcję **Szyfrowanie dysków funkcją BitLocker**.
7. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zaszyfruj wszystkie dyski twarde**.

Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po szyfrowaniu będziesz mógł załadować tylko ten system operacyjny, na którym szyfrowanie zostało wykonane.

8. Skonfiguruj zaawansowane opcje szyfrowania dysków funkcją BitLocker (patrz tabela poniżej).
9. Zapisz swoje zmiany.

[Jak uruchomić szyfrowanie dysków funkcją BitLocker za pośrednictwem konsoli Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, dla których chcesz uruchomić szyfrowanie dysków funkcją BitLocker.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
5. W sekcji **Zarządzaj szyfrowaniem** wybierz **Szyfrowanie dysków funkcją BitLocker**.
6. Kliknij odnośnik **Szyfrowanie dysków funkcją BitLocker**.
Spowoduje to otwarcie okna ustawień szyfrowania dysków funkcją Bitlocker.
7. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Zaszyfruj wszystkie dyski twarde**.

Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po szyfrowaniu będziesz mógł załadować tylko ten system operacyjny, na którym szyfrowanie zostało wykonane.

8. Skonfiguruj zaawansowane opcje szyfrowania dysków funkcją BitLocker (patrz tabela poniżej).
9. Kliknij **OK**.

Możesz użyć narzędzia Monitor szyfrowania, aby kontrolować szyfrowanie dysku lub proces deszyfrowania na komputerze użytkownika. Możesz uruchomić narzędzie Monitor szyfrowania z poziomu [okna głównego aplikacji](#).

Po zastosowaniu zasady aplikacja wyświetli następujące zapytania w zależności od ustawień uwierzytelniania:

- Tylko TPM. Wprowadzanie przez użytkownika nie jest wymagane. Dysk zostanie zaszyfrowany po ponownym uruchomieniu komputera.
- TPM + PIN / Hasło. Jeśli moduł TPM jest dostępny, pojawi się konto z prośbą o podanie kodu PIN. Jeśli moduł TPM nie jest dostępny, pojawi się okno z prośbą o wpisanie hasła do autoryzacji przed rozruchem.
- Tylko hasło. Zostanie wyświetlone okno z prośbą o wpisanie hasła do autoryzacji przed rozruchem.

Jeśli w systemie operacyjnym komputera jest włączona funkcja zgodności ze standardami FIPS (Federal Information Processing Standard), wówczas w systemie Windows 8 i wcześniejszych wersjach będzie wyświetlane okno z żądaniem podłączenia urządzenia magazynującego w celu zapisania pliku klucza odzyskiwania. Możesz zapisać kilka plików kluczy odzyskiwania na jednym urządzeniu magazynującym.

Po ustawieniu hasła lub kodu PIN funkcja BitLocker poprosi o ponowne uruchomienie komputera w celu dokończenia szyfrowania. Następnie użytkownik musi przejść procedurę uwierzytelniania funkcją BitLocker. Po procedurze uwierzytelnienia użytkownik musi zalogować się do systemu. Po załadowaniu systemu operacyjnego funkcja BitLocker zakończy szyfrowanie.

Jeśli nie ma dostępu do kluczy szyfrowania, użytkownik może [poprosić administratora sieci lokalnej o dostarczenie klucza odzyskiwania](#) (jeśli klucz odzyskiwania nie został wcześniej zapisany na urządzeniu magazynującym lub został utracony).

Ustawiania modułu Szyfrowania dysków funkcją BitLocker

Parametr	Opis
Włącz korzystanie z uwierzytelniania BitLocker wymagającego wprowadzania danych z klawiatury przed uruchomieniem na tabletach	<p>To pole włącza / wyłącza korzystanie z uwierzytelniania wymagającego wprowadzenia danych przed rozruchem nawet wtedy, gdy platforma nie oferuje takiej możliwości (na przykład klawiatury dotykowe na tabletach).</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"><p>Ekran dotykowy komputerów typu tablet nie jest dostępny w środowisku wykonawczym przed uruchomieniem systemu. Aby zakończyć uwierzytelnianie funkcji BitLocker na komputerach typu tablet, użytkownik musi, na przykład, podłączyć klawiaturę USB.</p></div> <p>Jeśli pole jest zaznaczone, użycie uwierzytelniania wymagającego wprowadzenia danych przed rozruchem jest dozwolone. Zalecane jest korzystanie z tego ustawienia tylko na urządzeniach, na których znajdują się alternatywne narzędzia do wprowadzania danych przed rozruchem, na przykład klawiatura USB będąca dodatkiem do klawiatury dotykowej.</p> <p>Jeśli pole jest odznaczone, szyfrowanie dysków funkcją BitLocker nie jest możliwe na tabletach.</p>
Użyj szyfrowania sprzętowego (dla systemu operacyjnego Windows 8 i nowszych)	<p>Jeśli pole jest zaznaczone, aplikacja stosuje szyfrowanie sprzętu. Umożliwia to przyspieszenie szyfrowania i zużycie mniejszej ilości zasobów.</p>
Szyfruj tylko zajętą przestrzeń dysku (dla)	<p>To pole włącza/wyłącza opcję ograniczającą obszar szyfrowania tylko do zajmowanych sektorów dysku twardego. To ograniczenie pozwala na skrócenie czasu szyfrowania.</p>

systemu operacyjnego
Windows 8 i nowszych)

Włączenie lub wyłączenie funkcji **Szyfruj tylko zajęta przestrzeń dysku (redukuje czas szyfrowania)** po rozpoczęciu szyfrowania nie powoduje zmodyfikowania tego ustawienia, aż do odszyfrowania dysków twardego. Przed rozpoczęciem szyfrowania należy zaznaczyć lub odznaczyć to pole.

Jeśli pole jest zaznaczone, zostaną zaszyfrowane tylko te obszary dysku twardego, które są zajęte przez pliki. Kaspersky Endpoint Security automatycznie szyfruje nowe dane po ich dodaniu.

Jeśli pole jest odznaczone, cały dysk twardego jest szyfrowany, w tym fragmenty wcześniej usuniętych i zmodyfikowanych plików.

Ta opcja jest zalecana dla nowych dysków twardego, których dane nie zostały zmodyfikowane ani usunięte. Jeśli stosujesz szyfrowanie na dysku twardego, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku twardego. Zapewni to ochronę wszystkich danych, także tych usuniętych, które potencjalnie można odzyskać.

Domyślnie pole to nie jest zaznaczone.

Ustawienia
uwierzytelniania

Użyj hasła (dla systemu operacyjnego Windows 8 i nowszych)

Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security wyświetli pytanie o wprowadzenie hasła podczas próby uzyskania dostępu do zaszyfrowanego dysku.

Ta opcja może zostać wybrana, gdy moduł TPM nie jest używany.

Używaj modułu TPM (Trusted Platform Module)

Jeśli ta opcja jest zaznaczona, BitLocker korzysta z modułu TPM (Trusted Platform Module).

Moduł TPM (Trusted Platform Module) to mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład, do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej.

Dla komputerów działających pod kontrolą systemu Windows 7 lub Windows Server 2008 R2 dostępne jest tylko szyfrowanie przy użyciu modułu TPM. Jeśli moduł TPM nie jest zainstalowany, szyfrowanie funkcją BitLocker nie jest możliwe. Użycie hasła na tych komputerach nie jest obsługiwane.

Urządzenie posiadające moduł Trusted Platform Module może tworzyć klucze szyfrowania, które mogą zostać odszyfrowane tylko z pomocą urządzenia. TPM szyfruje klucze szyfrowania, korzystając z własnych kluczy głównych magazynowania. Klucz główny magazynowania jest przechowywany w Trusted Platform Module. Zapewnia to dodatkowy poziom ochrony przed próbami zhakowania kluczy szyfrowania.

To ustawienie jest wybrane domyślnie.

Możesz ustawić dodatkową warstwę ochrony dostępu do klucza szyfrowania i zaszyfrować klucz z hasłem lub kodu PIN:

- **Użyj kodu PIN dla TPM.** Jeśli to pole jest zaznaczone, użytkownik może użyć kodu PIN do uzyskania dostępu do klucza szyfrowania przechowywanego w Trusted Platform Module (TPM).

Jeśli to pole jest odznaczone, użytkownicy nie mogą korzystać z kodów PIN. Aby uzyskać dostęp do klucza szyfrowania, użytkownik musi wprowadzić hasło.

Możesz zezwolić użytkownikowi na użycie rozszerzonego kodu PIN.

Rozszerzony kod PIN umożliwia używanie innych znaków jako dodatku do znaków numerycznych: dużych i małych liter alfabetu łacińskiego, znaków specjalnych i spacji.

- **Używaj modułu TPM (Trusted Platform Module); jeśli jest niedostępny - używaj hasła.** Jeśli pole jest zaznaczone, użytkownik może użyć hasła w celu uzyskania dostępu do kluczy szyfrowania, gdy moduł Trusted Platform Module (TPM) jest niedostępny.

Jeśli pole wyboru zostanie odznaczone, a TPM nie jest dostępny, szyfrowanie całego dysku nie rozpocznie się.

Deszyfrowanie dysku twardego chronionego przez funkcję BitLocker

Użytkownicy mogą odszyfrować dysk za pomocą systemu operacyjnego (funkcja *Wyłącz funkcję BitLocker*). Następnie Kaspersky Endpoint Security poprosi użytkownika o ponowne zaszyfrowanie dysku. Kaspersky Endpoint Security będzie monitorował o zaszyfrowanie dysku, chyba że włączysz deszyfrowanie dysku w zasadzie.

[Jak odszyfrować dysk twardy chroniony funkcją BitLocker za pomocą Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
6. Z listy rozwijalnej **Technologia szyfrowania** wybierz opcję **Szyfrowanie dysków funkcją BitLocker**.
7. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Odszyfruj wszystkie dyski twarde**.
8. Zapisz swoje zmiany.

[Jak odszyfrować dysk twardy zaszyfrowany przy pomocy funkcji BitLocker w Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz zakładkę **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, dla których chcesz odszyfrować dyski twarde.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Szyfrowanie danych** → **Szyfrowanie całego dysku**.
5. Wybierz technologię **Szyfrowanie dysków funkcją BitLocker** i kliknij odnośnik, aby skonfigurować ustawienia.
Ustawienia szyfrowania zostaną otwarte.
6. Z listy rozwijalnej **Tryb szyfrowania** wybierz **Odszyfruj wszystkie dyski twarde**.
7. Kliknij **OK**.

Możesz użyć narzędzia Monitor szyfrowania, aby kontrolować szyfrowanie dysku lub proces deszyfrowania na komputerze użytkownika. Możesz uruchomić narzędzie Monitor szyfrowania z poziomu [okna głównego aplikacji](#).

Przywracanie dostępu do dysku chronionego funkcją BitLocker

Jeśli użytkownik zapomniał hasła dostępu do dysku twardego zaszyfrowanego przez BitLocker, musisz rozpocząć procedurę odzyskiwania (Żądanie-Odpowiedź).

Jeśli system operacyjny komputera posiada włączony tryb kompatybilności FIPS (Federal Information Processing), wówczas w systemie Windows 8 i starszych plik klucza odzyskiwania jest zapisywany na nośniku wymiennym przed szyfrowaniem. Aby odzyskać dostęp do dysku, włóż nośnik wymienny i postępuj zgodnie z instrukcjami na ekranie.

Przywrócenie dostępu do dysku twardego zaszyfrowanego przez BitLocker składa się z następujących kroków:

1. Użytkownik informuje administratora o identyfikatorze klucza odzyskiwania (patrz rysunek poniżej).
2. Administrator weryfikuje identyfikator klucza odzyskiwania we właściwościach komputera w Kaspersky Security Center. Identyfikator podany przez użytkownika musi być zgodny z identyfikatorem wyświetlanym we właściwościach komputera.
3. Jeśli identyfikatory klucza odzyskiwania są zgodne, administrator dostarcza użytkownikowi klucz odzyskiwania lub wysyła plik klucza odzyskiwania.

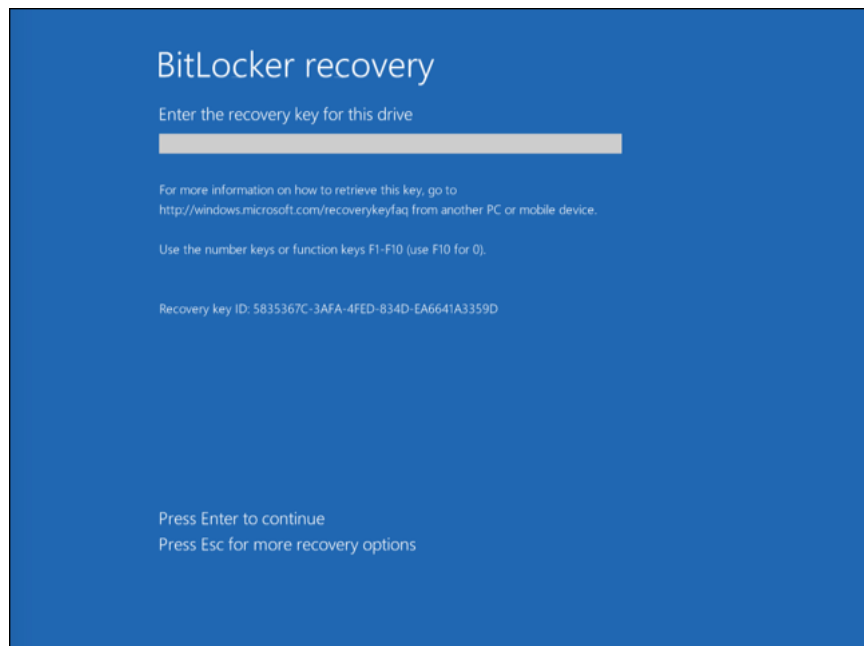
Plik klucza odzyskiwania jest używany dla komputerów z następującymi systemami operacyjnymi:

- Windows 7;
- Windows 8;
- Windows Server 2008;
- Windows Server 2011;

- Windows Server 2012.

W przypadku wszystkich innych systemów operacyjnych używany jest klucz odzyskiwania.

4. Użytkownik wprowadza klucz odzyskiwania i uzyskuje dostęp do dysku twardego.



Przywracanie dostępu do dysku systemowego zaszyfrowanego funkcją BitLocker

Przywracanie dostępu do dysku systemowego

Aby rozpocząć procedurę odzyskiwania, użytkownik musi wcisnąć klawisz **Esc** na etapie uwierzytelniania przed uruchomieniem.

[Jak wyświetlić klucz odzyskiwania dla dysku systemowego zaszyfrowanego przy pomocy funkcji BitLocker w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Na zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy.
5. Z menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.
6. W oknie, które zostanie otwarte, wybierz zakładkę **Dostęp do dysku systemowego chronionego funkcją BitLocker**.
7. Zapytaj użytkownika o ID klucza odzyskiwania wskazany w oknie do wprowadzenia hasła do funkcji BitLocker, a następnie porównaj go z ID w polu **ID klucza odzyskiwania**.

Jeśli numery ID nie pasują do siebie, ten klucz nie służy do przywrócenia dostępu do określonego dysku systemowego. Upewnij się, że nazwa wybranego komputera odpowiada nazwie komputera użytkownika.

W rezultacie będziesz mieć dostęp do klucza odzyskiwania lub pliku klucza odzyskiwania, który będzie musiał zostać przesłany do użytkownika.

[Jak wyświetlić klucz odzyskiwania dla dysku systemowego zaszyfrowanego przy pomocy funkcji BitLocker w konsoli Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Zaznacz pole wyboru obok nazwy komputera, do dysku którego chcesz przywrócić dostęp.
3. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.
4. W otwartym oknie wybierz sekcję **BitLocker**.
5. Sprawdź identyfikator klucza odzyskiwania. Identyfikator podany przez użytkownika musi być zgodny z identyfikatorem wyświetlanym w ustawieniach komputera.

Jeśli numery ID nie pasują do siebie, ten klucz nie służy do przywrócenia dostępu do określonego dysku systemowego. Upewnij się, że nazwa wybranego komputera odpowiada nazwie komputera użytkownika.

6. Kliknij przycisk **Uzyskaj klucz**.

W rezultacie będziesz mieć dostęp do klucza odzyskiwania lub pliku klucza odzyskiwania, który będzie musiał zostać przesłany do użytkownika.

Po załadowaniu systemu operacyjnego program Kaspersky Endpoint Security wyświetli monit o zmianę hasła lub kodu PIN. Po ustawieniu nowego hasła lub kodu PIN, funkcja BitLocker utworzy nowy klucz główny i wyśle go do Kaspersky Security Center. W wyniku tego działania klucz odzyskiwania oraz plik klucza odzyskiwania zostaną zaktualizowane. Jeśli użytkownik nie zmienił hasła, możesz użyć starego klucza odzyskiwania przy następnym ładowaniu systemu operacyjnego.

Komputery z systemem Windows 7 nie pozwalają na zmianę hasła lub kodu PIN. Po wprowadzeniu klucza odzyskiwania i załadowaniu systemu operacyjnego, program Kaspersky Endpoint Security nie wyświetli monitu o zmianę hasła lub kodu PIN. Dlatego też niemożliwe jest ustawienie nowego hasła lub kodu PIN. Ten problem jest spowodowany przez szczególne właściwości systemu operacyjnego. Aby kontynuować, należy ponownie zaszyfrować dysk twardy.

Przywracanie dostępu do dysku niesystemowego

Aby rozpocząć procedurę odzyskiwania, użytkownik musi kliknąć odnośnik **Nie pamiętam hasła** w oknie zapewniającym dostęp do dysku. Po uzyskaniu dostępu do zaszyfrowanego dysku, użytkownik może włączyć automatyczne odblokowywanie dysku podczas uwierzytelniania systemu Windows w ustawieniach funkcji BitLocker.

[Jak wyświetlić klucz odzyskiwania dla dysku niesystemowego zaszyfrowanego przez funkcję BitLocker w Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz kolejno **Dodatkowe** → **Ochrona i szyfrowanie danych** → **Zaszyfrowane dyski**.
3. W obszarze roboczym wybierz zaszyfrowane urządzenie, dla którego chcesz utworzyć plik klucza dostępu, a z menu kontekstowego urządzenia wybierz **Uzyskaj dostęp do urządzenia z poziomu Kaspersky Endpoint Security for Windows**.
4. Zapytaj użytkownika o ID klucza odzyskiwania wskazany w oknie do wprowadzenia hasła do funkcji BitLocker, a następnie porównaj go z ID w polu **ID klucza odzyskiwania**.

Jeśli numery ID nie pasują do siebie, ten klucz nie służy do przywrócenia dostępu do określonego dysku. Upewnij się, że nazwa wybranego komputera odpowiada nazwie komputera użytkownika.

5. Wyślij do użytkownika klucz, który jest wskazany w polu **klucz odzyskiwania**.

[Jak wyświetlić klucz odzyskiwania dla dysku niesystemowego zaszyfrowanego przy pomocy funkcji BitLocker w konsoli Web Console i Cloud Console?](#)

1. W oknie głównym konsoli Web Console wybierz **Operacje** → **Szyfrowanie i ochrona danych** → **Zaszyfrowane dyski**.

2. Zaznacz pole wyboru obok nazwy komputera, do dysku którego chcesz przywrócić dostęp.

3. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.

Spowoduje to uruchomienie Kreatora umożliwiającego uzyskanie dostępu do urządzenia.

4. Postępuj zgodnie z instrukcjami Kreatora, aby przyznać dostęp do urządzenia:

a. Wybierz wtyczkę **Kaspersky Endpoint Security for Windows**.

b. Sprawdź identyfikator klucza odzyskiwania. Identyfikator podany przez użytkownika musi być zgodny z identyfikatorem wyświetlanym w ustawieniach komputera.

Jeśli numery ID nie pasują do siebie, ten klucz nie służy do przywrócenia dostępu do określonego dysku systemowego. Upewnij się, że nazwa wybranego komputera odpowiada nazwie komputera użytkownika.

c. Kliknij przycisk **Uzyskaj klucz**.

W rezultacie będziesz mieć dostęp do klucza odzyskiwania lub pliku klucza odzyskiwania, który będzie musiał zostać przesłany do użytkownika.

Wstrzymywanie ochrony funkcją BitLocker w celu zaktualizowania oprogramowania

Istnieje liczba kwestii specjalnych dla aktualizacji systemu operacyjnego, instalacji pakietów aktualizacji dla systemu operacyjnego lub aktualizacji innego oprogramowania z włączoną ochroną funkcją BitLocker. Instalowanie aktualizacji może wymagać ponownego uruchomienia komputera kilka razy. Po każdym ponownym uruchomieniu użytkownik musi zakończyć uwierzytelnianie funkcji BitLocker. Aby poprawnie zainstalować aktualizacje, możesz tymczasowo wyłączyć uwierzytelnianie funkcji BitLocker. W tym przypadku dysk pozostaje zaszyfrowany, a użytkownik posiada dostęp do danych po zalogowaniu do systemu. Aby zarządzać uwierzytelnianiem funkcji BitLocker, musisz użyć zadania *Zarządzanie ochroną BitLocker*. Możesz użyć tego zadania do określenia liczby ponownych uruchomień komputera, które nie wymagają uwierzytelniania funkcji BitLocker. W ten sposób, po zainstalowaniu aktualizacji i zakończeniu zadania *Zarządzanie ochroną BitLocker*, uwierzytelnianie funkcji BitLocker jest automatycznie włączone. Możesz wyłączyć uwierzytelnianie funkcji BitLocker w dowolnym momencie.

[Jak wstrzymać ochronę BitLocker przy użyciu Konsoli administracyjnej \(MMC\)?](#) 

1. W Konsoli administracyjnej przejdź do folderu **Serwer administracyjny** → **Zadania**.

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Nowe zadanie**.

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

Krok 1. Wybieranie typu zadania

Wybierz **Kaspersky Endpoint Security for Windows (11.7.0)** → **Zarządzanie ochroną BitLocker**.

Krok 2. Zarządzanie ochroną Bitlocker

Skonfiguruj uwierzytelnianie funkcji BitLocker. Aby wstrzymać ochronę BitLocker, wybierz **Tymczasowo zezwól na pomijanie uwierzytelniania funkcji BitLocker** i wprowadź liczbę ponownych uruchomień bez uwierzytelniania funkcji BitLocker (1 do 15 razy). Jeśli to konieczne, wprowadź datę i godzinę wygaśnięcia zadania. O określonej godzinie zadanie jest automatycznie wyłączone, a użytkownik musi zakończyć uwierzytelnianie funkcji BitLocker po ponownym uruchomieniu komputera.

Krok 3. Wybieranie urządzeń, do których zostanie przypisane zadanie

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

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

Krok 4. Definiowanie nazwy zadania

Wprowadź nazwę zadania, na przykład, **Aktualizowanie do Windows 10**.

Krok 5. Kończenie tworzenia zadania

Zakończ działanie Kreatora. W razie potrzeby zaznacz pole **Uruchom zadanie po zakończeniu działania kreatora**. Możesz monitorować postęp zadania we właściwościach zadania.

[Jak wstrzymać ochronę BitLocker przy użyciu konsoli Web Console?](#) 

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

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

Krok 1. Konfigurowanie ogólnych ustawień zadania

Skonfiguruj ogólne ustawienia zadania:

1. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

2. Na liście rozwijanej **Typ zadania** wybierz **Zarządzanie ochroną BitLocker**.

3. W polu **Nazwa zadania** wpisz krótki opis, na przykład, **Aktualizowanie do Windows 10**.

4. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

Krok 2. Zarządzanie ochroną BitLocker

Skonfiguruj uwierzytelnianie funkcji BitLocker. Aby wstrzymać ochronę BitLocker, wybierz **Tymczasowo zezwól na pomijanie uwierzytelniania funkcji BitLocker** i wprowadź liczbę ponownych uruchomień bez uwierzytelniania funkcji BitLocker (1 do 15 razy). Jeśli to konieczne, wprowadź datę i godzinę wygaśnięcia zadania. O określonej godzinie zadanie jest automatycznie wyłączone, a użytkownik musi zakończyć uwierzytelnianie funkcji BitLocker po ponownym uruchomieniu komputera.

Krok 3. Kończenie tworzenia zadania

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

Aby uruchomić zadanie, zaznacz pole obok zadania i kliknij przycisk **Uruchom**.

W wyniku tego działania, podczas uruchamiania zadani, po kolejnym ponownym uruchomieniu komputera, BitLocker nie wyświetli pytania o autoryzację. Po każdym ponownym uruchomieniu komputera bez uwierzytelnienia funkcji BitLocker, Kaspersky Endpoint Security wygeneruje odpowiednie zdarzenie i zarejestruje liczbę pozostałych ponownych uruchomień. Następnie Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center do monitorowania przez administratora. Możesz także znaleźć liczbę pozostałych ponownych uruchomień we właściwościach komputera, w konsoli Kaspersky Security Center.

Jeśli określona liczba ponownych uruchomień lub czas wygaśnięcia zadania zostaną osiągnięte, uwierzytelnianie funkcji BitLocker zostanie automatycznie włączone. Aby uzyskać dostęp do danych, użytkownik musi zakończyć uwierzytelnianie funkcji BitLocker.

Na komputerach działających pod kontrolą systemu Windows 7, BitLocker nie może zliczać ponownych uruchomień komputera. Zliczanie ponownych uruchomień na komputerach z systemem Windows 7 jest zarządzane przez Kaspersky Endpoint Security. Dlatego też, aby uwierzytelnianie funkcji BitLocker było automatycznie włączone po każdym ponownym uruchomieniu, należy uruchomić Kaspersky Endpoint Security.

Aby włączyć uwierzytelnianie funkcji BitLocker z wyprzedzeniem, otwórz właściwości zadania *Zarządzanie ochroną BitLocker* i zaznacz opcję **Żądaj uwierzytelnienia za każdym razem przed rozruchem**.

Szyfrowanie na poziomie plików na lokalnych dyskach komputera

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Szyfrowanie plików ma następujące funkcje specjalne:

- Kaspersky Endpoint Security szyfruje / deszyfruje pliki w wstępnie określonych folderach tylko dla profili lokalnego użytkownika systemu operacyjnego. Kaspersky Endpoint Security nie szyfruje / deszyfruje plików w predefiniowanych folderach profili użytkownika mobilnego, obowiązkowych profili użytkownika, tymczasowych profili użytkownika lub folderach przekierowanych.
- Kaspersky Endpoint Security nie szyfruje plików, których modyfikacja mogłaby uszkodzić system operacyjny i zainstalowane aplikacje. Na przykład, na liście wykluczeń szyfrowania znajdują się następujące pliki i foldery ze wszystkimi osadzonymi folderami:
 - %WINDIR%;
 - %PROGRAMFILES% i %PROGRAMFILES(X86)%;
 - Pliki rejestru systemu Windows.

Lista wykluczeń z szyfrowania nie może być podglądana ani modyfikowana. Pliki i foldery znajdujące się na liście wykluczeń z szyfrowania mogą być dodawane do listy szyfrowania, ale i tak nie będą szyfrowane podczas wykonywania szyfrowania plików.

Szyfrowanie plików na lokalnych dyskach komputera

Kaspersky Endpoint Security nie szyfruje plików, których zawartość znajduje się w magazynie w chmurze OneDrive, i blokuje kopiowanie zaszyfrowanych plików do magazynu w chmurze OneDrive, jeśli te pliki nie zostają dodane do [reguły odszyfrowania](#).

W celu zaszyfrowania plików na dyskach lokalnych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie plików**.

6. W prawej części okna wybierz zakładkę **Szyfrowanie**.

7. Z listy rozwijalnej **Tryb szyfrowania** wybierz element **Zgodnie z regułami**.

8. Na zakładce **Szyfrowanie** kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz jeden z następujących elementów:

- a. Wybierz element **Wstępnie określone foldery**, aby dodać pliki z folderów lokalnych profili użytkowników, zasugerowanych przez specjalistów z Kaspersky, do reguły szyfrowania.
- **Dokumenty**. Pliki w standardowym folderze *Dokumenty* systemu operacyjnego i jego podfolderach.
 - **Ulubione**. Pliki w standardowym folderze *Ulubione* systemu operacyjnego i jego podfolderach.
 - **Pulpit**. Pliki w standardowym folderze *Pulpit* systemu operacyjnego i jego podfolderach.
 - **Pliki tymczasowe**. Pliki tymczasowe związane z działaniem aplikacji zainstalowanych na komputerze. Na przykład, aplikacje Microsoft Office tworzą pliki tymczasowe zawierające kopie zapasowe dokumentów.
 - **Pliki programu Outlook**. Pliki dotyczące działania klienta poczty Outlook: pliki danych (PST), pliki danych offline (OST), pliki książki adresowej offline (OAB) oraz pliki osobistej książki adresowej (PAB).

b. Wybierz element **Folder niestandardowy**, aby dodać ręcznie wprowadzoną ścieżkę folderu do reguły szyfrowania.

Dodając ścieżkę folderu, przestrzegaj następujących zasad:

- Użyj zmiennej środowiskowej (na przykład: %FOLDER%\UserFolder\). Możesz użyć zmiennej środowiskowej tylko raz i tylko na początku ścieżki.
- Nie używaj ścieżek względnych. Możesz użyć zestawu `\..\` (np. C:\Users\..\UserFolder\). Zestaw `\..\` oznacza przejście do folderu nadrzędnego.
- Nie używaj znaków `*` i `?`.
- Nie używaj ścieżek UNC.
- Użyj `;` lub `,` jako separatora.

c. Wybierz element **Pliki według rozszerzenia**, aby dodać rozszerzenia pojedynczych plików do reguły szyfrowania. Kaspersky Endpoint Security zaszyfruje pliki z określonymi rozszerzeniami na wszystkich lokalnych dyskach komputera.

d. Wybierz element **Pliki według grup rozszerzeń**, aby dodać grupy rozszerzeń plików do reguły szyfrowania (na przykład: *Dokumenty Microsoft Office*). Kaspersky Endpoint Security szyfruje pliki, które mają rozszerzenia znajdujące się na liście grup rozszerzeń na wszystkich lokalnych dyskach komputera.

9. Zapisz swoje zmiany.

Natychmiast po zastosowaniu profilu program Kaspersky Endpoint Security szyfruje te pliki, które znajdują się w regule szyfrowania, a nie znajdują się w [regule deszyfrowania](#).

Szyfrowanie plików ma następujące funkcje specjalne:

- Jeśli ten sam plik zostanie dodany zarówno do reguły szyfrowania, jak i reguły deszyfrowania, wówczas Kaspersky Endpoint Security wykonuje następujące działania:
 - Jeśli plik nie jest zaszyfrowany, Kaspersky Endpoint Security nie szyfruje tego pliku.

- Jeśli plik jest zaszyfrowany, Kaspersky Endpoint Security odszyfrowuje ten plik.
- Kaspersky Endpoint Security kontynuuje szyfrowanie nowych plików, jeśli pliki te spełniają kryteria reguły szyfrowania. Na przykład, po zmianie właściwości niezasyfrowanego pliku (ścieżki lub rozszerzenia) plik spełnia kryteria reguły szyfrowania. Kaspersky Endpoint Security szyfruje ten plik.
- Jeśli użytkownik tworzy nowy plik, którego właściwości spełniają kryteria reguły szyfrowania, Kaspersky Endpoint Security szyfruje plik, gdy tylko zostanie on otwarty.
- Kaspersky Endpoint Security odradza szyfrowanie otwartych plików, aż do ich zamknięcia.
- Jeśli przeniesiesz zaszyfrowany plik do innego folderu na dysku lokalnym, plik pozostanie zaszyfrowany bez względu na to, czy ten folder znajduje się w regule szyfrowania.
- Jeśli odszyfrujesz plik i skopiujesz go do innego folderu lokalnego, który nie jest objęty regułą deszyfrowania, kopia pliku może zostać zaszyfrowana. Aby zapobiec szyfrowaniu kopiowanego pliku, utwórz regułę deszyfrowania folderu docelowego.

Tworzenie reguł dostępu do zaszyfrowanego pliku dla aplikacji

W celu utworzenia reguł dostępu do zaszyfrowanego pliku dla aplikacji:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie plików**.
6. W prawej części okna wybierz zakładkę **Szyfrowanie**.
7. Z listy rozwijalnej **Tryb szyfrowania** wybierz element **Zgodnie z regułami**.

Reguły dostępu są stosowane tylko w trybie **Zgodnie z regułami**. Po zastosowaniu reguł dostępu w trybie **Zgodnie z regułami**, jeśli zmienisz na tryb **Pozostaw niezmienione**, Kaspersky Endpoint Security będzie ignorował wszystkie reguły dostępu. Wszystkie aplikacje będą miały dostęp do wszystkich zaszyfrowanych plików.

8. W prawej części okna wybierz zakładkę **Reguły dla aplikacji**.
9. Jeśli chcesz wybrać aplikacje wyłącznie z listy Kaspersky Security Center, kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz element **Aplikacje z listy Kaspersky Security Center**.
 - a. Określ filtry w celu zawężenia listy aplikacji w tabeli. W tym celu określ wartości parametrów **Aplikacja**, **Producent** i **Okres dodania** oraz wszystkich pól z sekcji **Grupa**.
 - b. Kliknij przycisk **Odśwież**.

- c. Tabela wyświetla aplikacje, które odpowiadają stosowanym filtrom.
- d. W kolumnie **Aplikacje** zaznacz pola obok aplikacji, dla których chcesz utworzyć reguły dostępu do zaszyfrowanych plików.
- e. Z listy rozwijalnej **Reguła dla aplikacji** wybierz regułę, która będzie determinować dostęp aplikacji do zaszyfrowanych plików.
- f. Z listy rozwijalnej **Działania dla aplikacji wybranych wcześniej** wybierz działanie, jakie Kaspersky Endpoint Security podejmie na regułach dostępu do zaszyfrowanego pliku, które zostały wcześniej utworzone dla tych aplikacji.

Szczegółowe informacje o regule dostępu do zaszyfrowanego pliku dla aplikacji pojawią się w tabeli, na zakładce **Reguły dla aplikacji**.

10. Jeżeli chcesz ręcznie wybrać aplikacje, kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz element **Niestandardowe aplikacje**.

- a. W polu do wprowadzania danych wpisz nazwę lub listę nazw plików wykonywalnych, w tym ich rozszerzenia. Możesz także dodać nazwy plików wykonywalnych aplikacji z listy Kaspersky Security Center poprzez kliknięcie przycisku **Dodaj z listy Kaspersky Security Center**.
- b. Jeśli to konieczne, w polu **Opis** wprowadź opis listy aplikacji.
- c. Z listy rozwijalnej **Reguła dla aplikacji** wybierz regułę, która będzie determinować dostęp aplikacji do zaszyfrowanych plików.

Szczegółowe informacje o regule dostępu do zaszyfrowanego pliku dla aplikacji pojawią się w tabeli, na zakładce **Reguła dla aplikacji**.

11. Zapisz swoje zmiany.

Szyfrowanie plików utworzonych lub zmodyfikowanych przez określone aplikacje

Możesz utworzyć regułę, według której Kaspersky Endpoint Security będzie szyfrować pliki utworzone lub zmodyfikowane przez aplikacje określone w regule.

Pliki utworzone lub zmodyfikowane przez określone aplikacje przed zastosowaniem reguły szyfrowania nie zostaną zaszyfrowane.

W celu skonfigurowania szyfrowania plików utworzonych lub zmodyfikowanych przez określone aplikacje:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.

5. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie plików**.
6. W prawej części okna wybierz zakładkę **Szyfrowanie**.
7. Z listy rozwijalnej **Tryb szyfrowania** wybierz element **Zgodnie z regułami**.

Reguły szyfrowania są stosowane tylko w trybie **Zgodnie z regułami**. Po zastosowaniu reguł szyfrowania w trybie **Zgodnie z regułami**, jeśli zmienisz na tryb **Pozostaw niezmiennione**, Kaspersky Endpoint Security będzie ignorował wszystkie reguły szyfrowania. Pliki, które zostały wcześniej zaszyfrowane, pozostaną zaszyfrowane.

8. W prawej części okna wybierz zakładkę **Reguły dla aplikacji**.
9. Jeśli chcesz wybrać aplikacje wyłącznie z listy Kaspersky Security Center, kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz element **Aplikacje z listy Kaspersky Security Center**.
 - a. Określ filtry w celu zawężenia listy aplikacji w tabeli. W tym celu określ wartości parametrów **Aplikacja**, **Producent** i **Okres dodania** oraz wszystkich pól z sekcji **Grupa**.
 - b. Kliknij przycisk **Odśwież**.

Tabela wyświetla aplikacje, które odpowiadają stosowanym filtrom.
 - c. W kolumnie **Aplikacje** zaznacz pola obok aplikacji, których utworzone pliki mają być zaszyfrowane.
 - d. Z listy rozwijalnej **Reguła dla aplikacji** wybierz **Zaszyfruj wszystkie utworzone pliki**.
 - e. Z listy rozwijalnej **Działania dla aplikacji wybranych wcześniej** wybierz działanie, jakie Kaspersky Endpoint Security podejmie na regułach szyfrowania plików, które zostały wcześniej utworzone dla tych aplikacji.

Informacje o regule szyfrowania dla plików utworzonych lub zmodyfikowanych przez wybrane aplikacje pojawią się w tabeli na zakładce **Reguły dla aplikacji**.
10. Jeżeli chcesz ręcznie wybrać aplikacje, kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz element **Niestandardowe aplikacje**.
 - a. W polu do wprowadzania danych wpisz nazwę lub listę nazw plików wykonywalnych, w tym ich rozszerzenia.

Możesz także dodać nazwy plików wykonywalnych aplikacji z listy Kaspersky Security Center poprzez kliknięcie przycisku **Dodaj z listy Kaspersky Security Center**.
 - b. Jeśli to konieczne, w polu **Opis** wprowadź opis listy aplikacji.
 - c. Z listy rozwijalnej **Reguła dla aplikacji** wybierz **Zaszyfruj wszystkie utworzone pliki**.

Informacje o regule szyfrowania dla plików utworzonych lub zmodyfikowanych przez wybrane aplikacje zostaną wyświetlone w tabeli na zakładce **Reguła dla aplikacji**.
11. Zapisz swoje zmiany.

Generowanie reguły deszyfrowania

W celu wygenerowania reguły deszyfrowania:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie plików**.
6. W prawej części okna wybierz zakładkę **Odszyfrowywanie**.
7. Z listy rozwijalnej **Tryb szyfrowania** wybierz element **Zgodnie z regułami**.
8. Na zakładce **Odszyfrowywanie** kliknij przycisk **Dodaj** i z listy rozwijalnej wybierz jeden z następujących elementów:
 - a. Wybierz element **Wstępnie określone foldery**, aby dodać pliki z folderów lokalnych profili użytkowników, zasugerowanych przez specjalistów z Kaspersky, do reguły deszyfrowania.
 - b. Wybierz element **Folder niestandardowy**, aby dodać ręcznie wprowadzoną ścieżkę folderu do reguły deszyfrowania.
 - c. Wybierz element **Pliki według rozszerzenia**, aby dodać pojedyncze rozszerzenia plików do reguły deszyfrowania. Kaspersky Endpoint Security nie szyfruje plików z określonymi rozszerzeniami na wszystkich lokalnych dyskach komputera.
 - d. Wybierz element **Pliki według grup rozszerzeń**, aby dodać grupy rozszerzeń plików do reguły deszyfrowania (na przykład: *Dokumenty Microsoft Office*). Kaspersky Endpoint Security nie szyfruje plików, które mają rozszerzenia znajdujące się na liście grup rozszerzeń na wszystkich lokalnych dyskach komputera.
9. Zapisz swoje zmiany.

Jeśli ten sam plik został dodany do reguły szyfrowania oraz do reguły deszyfrowania, Kaspersky Endpoint Security nie zaszyfruje tego pliku, jeśli nie jest zaszyfrowany, a odszyfruje plik, jeśli jest zaszyfrowany.

Deszyfrowanie plików na lokalnych dyskach komputera

W celu odszyfrowania plików na dyskach lokalnych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Szyfrowanie danych** → **Szyfrowanie plików**.

6. W prawej części okna wybierz zakładkę **Szyfrowanie**.

7. Usuń z listy szyfrowania te pliki i foldery, które chcesz odszyfrować. W tym celu zaznacz pliki i wybierz element **Usuń regułę i odszyfruj pliki** z menu kontekstowego przycisku **Usuń**.

Możesz usunąć kilka elementów z listy zaszyfrowanych jednocześnie. W tym celu, trzymając wciśnięty klawisz **CTRL** zaznacz żądane pliki, klikając je lewym przyciskiem myszy, i wybierz element **Usuń regułę i odszyfruj pliki** z menu kontekstowego przycisku **Usuń**.

Pliki i foldery usuwane z listy zaszyfrowanych są automatycznie dodawane do listy odszyfrowanych.

8. [Utwórz listę deszyfrowanych plików](#).

9. Zapisz swoje zmiany.

Jak tylko profil zostanie zastosowany, Kaspersky Endpoint Security odszyfruje zaszyfrowane pliki, które zostały dodane do listy deszyfrowanych.

Kaspersky Endpoint Security deszyfruje zaszyfrowane pliki, jeśli ich parametry (ścieżka dostępu do pliku / nazwa pliku / rozszerzenie pliku) zostały zmienione, aby pasowały do parametrów obiektów dodanych do listy deszyfrowanych.

Kaspersky Endpoint Security odracza deszyfrację otwartych plików, aż do ich zamknięcia.

Tworzenie zaszyfrowanych pakietów

Aby chronić dane podczas wysyłania plików do użytkowników poza sieć korporacyjną, możesz użyć zaszyfrowanych pakietów. Zaszyfrowane pakiety mogą być wygodne do przesyłania plików o dużych rozmiarach na nośniki wymienne, gdyż klienci poczty e-mail posiadają ograniczenia rozmiaru plików.

Przed utworzeniem zaszyfrowanych pakietów Kaspersky Endpoint Security wyświetli pytanie o podanie hasła. Aby solidnie chronić dane, możesz włączyć sprawdzanie siły hasła oraz określić wymagania co do siły hasła. Uniemożliwi to użytkownikom korzystanie z krótkich i prostych haseł, na przykład: 1234.

[Jak włączyć sprawdzanie siły hasła podczas tworzenia zaszyfrowanych archiwów w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Szyfrowanie danych** → **Ogólne ustawienia szyfrowania**.
6. W sekcji **Ustawienia hasła** kliknij przycisk **Ustawienia**.
7. W otwartym oknie wybierz zakładkę **Zaszyfrowane pakiety**.
8. Podczas tworzenia zaszyfrowanych pakietów skonfiguruj ustawienia złożoności hasła.


1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz włączyć sprawdzanie siły hasła.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Szyfrowanie danych** → **Szyfrowanie plików**.
5. W sekcji **Ustawienia hasła pakietu zaszyfrowanego** skonfiguruj kryteria siły hasła wymagane podczas tworzenia zaszyfrowanych pakietów.

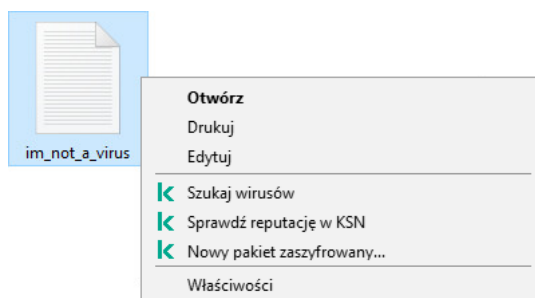
Możesz utworzyć zaszyfrowane pakiety na komputerach z zainstalowanym programem Kaspersky Endpoint Security z dostępnym Szyfrowaniem plików.

Podczas dodawania pliku do zaszyfrowanego pakietu, którego zawartość znajduje się w magazynie w chmurze OneDrive, Kaspersky Endpoint Security pobierze zawartość pliku i przeprowadzi szyfrowanie.

W celu utworzenia zaszyfrowanego pakietu:

1. W dowolnym menedżerze plików wybierz pliki lub foldery, które chcesz dodać do zaszyfrowanego pakietu. Kliknij je prawym przyciskiem myszy w celu otwarcia ich menu kontekstowego.
2. Z otwartego menu kontekstowego wybierz **Nowy pakiet zaszyfrowany** (patrz rysunek poniżej).
3. W otwartym oknie wybierz lokalizację na nośniku wymiennym, aby zapisać zaszyfrowany pakiet → określ nazwę pakietu i kliknij przycisk **Zapisz**.
4. W otwartym oknie określ hasło i potwierdź je.
Hasło musi spełniać złożone kryteria określone w zasadzie.
5. Kliknij przycisk **Utwórz**.

Zostanie uruchomiony proces tworzenia zaszyfrowanego pakietu. Podczas tworzenia zaszyfrowanego pakietu Kaspersky Endpoint Security nie przeprowadza kompresji plików. Po zakończeniu procesu, w wybranym folderze docelowym zostanie utworzony samorozpakowujący się zaszyfrowany pakiet chroniony hasłem (plik wykonywalny z rozszerzeniem .exe – ).



Tworzenie zaszyfrowanego pakietu

Aby uzyskać dostęp do plików w zaszyfrowanym pakiecie, kliknij go dwukrotnie, aby uruchomić Kreator rozpakowywania, a następnie wprowadź hasło. Jeśli zapomniałeś lub zgubiłeś swoje hasło, nie jest możliwe odzyskanie go i uzyskanie dostępu do plików w zaszyfrowanym pakiecie. Możesz ponownie utworzyć zaszyfrowany pakiet.

Przywracanie dostępu do zaszyfrowanych plików

Jeśli pliki są szyfrowane, Kaspersky Endpoint Security otrzymuje klucz szyfrowania wymagany do bezpośredniego dostępu do zaszyfrowanych plików. Użytkownik pracujący z poziomu dowolnego konta Windows, które było aktywne podczas szyfrowania pliku, może uzyskać bezpośredni dostęp do zaszyfrowanych plików, używając tego klucza szyfrowania. Użytkownicy pracujący z poziomu kont Windows, które były nieaktywne podczas szyfrowania pliku muszą być połączeni z Kaspersky Security Center w celu uzyskania dostępu do zaszyfrowanych plików.

Zaszyfrowane pliki mogą być niedostępne w następujących przypadkach:

- Na komputerze użytkownika przechowywane są klucze szyfrowania, ale nie ma połączenia z Kaspersky Security Center w celu zarządzania nimi. W tym przypadku użytkownik musi poprosić administratora lokalnej sieci firmowej o dostęp do zaszyfrowanych plików.

Jeśli nie ma dostępu do Kaspersky Security Center, należy:

- poprosić o klucz dostępu do plików zaszyfrowanych na dyskach twardych komputera;
- poprosić o oddzielne klucze dostępu dla zaszyfrowanych plików na każdym dysku wymiennym, aby móc uzyskać dostęp do zaszyfrowanych plików przechowywanych na nośnikach wymiennych.
- Moduły szyfrujące są usuwane z komputera użytkownika. W tej sytuacji użytkownik może otworzyć zaszyfrowane pliki na dyskach lokalnych i nośnikach wymiennych, ale zawartość tych plików będzie zaszyfrowana.

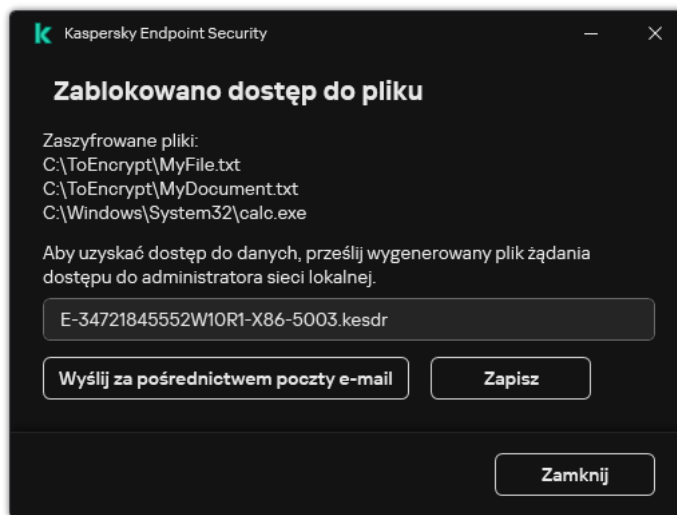
Użytkownik może pracować z zaszyfrowanymi plikami w następujących przypadkach:

- Pliki są umieszczane w [zaszyfrowanych pakietach](#) utworzonych na komputerze z zainstalowanym programem Kaspersky Endpoint Security.
- Pliki są przechowywane na nośnikach wymiennych, na których dozwolony jest [tryb przenośny](#).

Aby uzyskać dostęp do zaszyfrowanych plików, użytkownik musi rozpocząć procedurę odzyskiwania (Żądanie-Odpowiedź).

Odzyskiwanie dostępu do zaszyfrowanych plików składa się z następujących kroków:

1. Użytkownik wysła plik zawierający żądanie dostępu do administratora (patrz rysunek poniżej).
2. Administrator dodaje plik żądania dostępu do Kaspersky Security Center, tworzy plik klucza dostępu i wysyła ten plik do użytkownika.
3. Użytkownik dodaje plik klucza dostępu do Kaspersky Endpoint Security i uzyskuje dostęp do plików.



Przywracanie dostępu do zaszyfrowanych plików

Aby rozpocząć procedurę odzyskiwania, użytkownik musi spróbować uzyskać dostęp do pliku. W rezultacie Kaspersky Endpoint Security utworzy plik dostępu do żądania (plik z rozszerzeniem KESDC), który użytkownik musi wysłać administratorowi, na przykład, za pośrednictwem poczty elektronicznej.

Kaspersky Endpoint Security generuje plik zawierający żądanie dostępu do wszystkich zaszyfrowanych plików przechowywanych na dysku komputera (dysk lokalny lub dysk wymienny).

[Jak uzyskać zaszyfrowany plik klucza dostępu do danych w Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Na zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy.
5. Z menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.
6. W otwartym oknie wybierz zakładkę **Szyfrowanie danych**.
7. Na zakładce **Szyfrowanie danych** kliknij przycisk **Przełóżaj**.
8. W oknie wyboru pliku dostępu do żądania określ ścieżkę do pliku otrzymanego od użytkownika.

Zobaczysz informacje o żądaniu użytkownika. Kaspersky Security Center wygeneruje plik klucza. Wyślij do użytkownika wygenerowany plik klucza dostępu do zaszyfrowanych danych. Lub zapisz plik dostępu i użyj dowolnej dostępnej metody, aby przenieść plik.

[Jak uzyskać zaszyfrowany plik klucza dostępu do danych w konsoli Wen Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Zaznacz pole wyboru obok nazwy komputera, do którego danych chcesz przywrócić dostęp.
3. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.
4. Wybierz sekcję **Szyfrowanie danych**.
5. Kliknij przycisk **Wybierz plik** i wybierz plik żądania dostępu otrzymany od użytkownika (plik z rozszerzeniem KESDC).
Konsola Web Console wyświetli informacje o żądaniu. Obejmuje to nazwę komputera, na którym użytkownik żąda dostępu do pliku.
6. Kliknij przycisk **Zapisz klucz** i wybierz folder, aby zapisać plik klucza dostępu do zaszyfrowanych danych (plik z rozszerzeniem KESDR).

W rezultacie będziesz mógł uzyskać klucz dostępu do zaszyfrowanych danych, który będziesz musiał przekazać użytkownikowi.

Po otrzymaniu pliku klucza dostępu do zaszyfrowanych danych, użytkownik musi uruchomić plik, klikając go dwukrotnie. W rezultacie Kaspersky Endpoint Security zapewni dostęp do wszystkich zaszyfrowanych plików przechowywanych na dysku. Aby mieć dostęp do zaszyfrowanych plików przechowywanych na innych dyskach, należy uzyskać oddzielny plik klucza dostępu dla każdego dysku.

Przywracanie dostępu do zaszyfrowanych danych po awarii systemu operacyjnego

Możesz przywrócić dostęp do danych po błędzie systemu operacyjnego tylko dla szyfrowania na poziomie plików (FLE). Nie możesz przywrócić dostępu do danych, jeśli używane jest szyfrowanie całego dysku (FDE).

W celu przywrócenia dostępu do zaszyfrowanych danych po awarii systemu operacyjnego:

1. Przeinstaluj system operacyjny bez formatowania dysku twardego.
2. [Zainstaluj Kaspersky Endpoint Security](#).
3. Nawiąż połączenie między komputerem a Serwerem administracyjnym Kaspersky Security Center, który kontrolował komputer, gdy dane były zaszyfrowane.

Dostęp do zaszyfrowanych danych zostanie nadany na tych samych warunkach, które zostały zastosowane przed awarią systemu operacyjnego.

Modyfikowanie szablonów wiadomości dostępu do zaszyfrowanego pliku

W celu zmodyfikowania szablonów wiadomości dostępu do zaszyfrowanego pliku:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.

3. W obszarze roboczym wybierz zakładkę **Profile**.

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

5. W oknie zasady wybierz **Szyfrowanie danych** → **Ogólne ustawienia szyfrowania**.

6. W sekcji **Szablony** kliknij przycisk **Szablony**.

Zostanie otwarte okno **Szablony**.

7. Wykonaj następujące czynności:

- Jeśli chcesz zmodyfikować szablon wiadomości użytkownika, wybierz zakładkę **Komunikat użytkownika**. Okno **Dostęp do danych jest zablokowany** zostaje otwarte, gdy użytkownik próbuje uzyskać dostęp do zaszyfrowanego pliku, a na komputerze nie ma klucza dostępu do zaszyfrowanych plików. Kliknięcie przycisku **Wyślij przez e-mail** w oknie **Dostęp do danych jest zablokowany** powoduje automatyczne utworzenie wiadomości użytkownika. Wiadomość ta jest wysyłana do administratora korporacyjnej sieci LAN wraz z prośbą o dostęp do zaszyfrowanych plików.
- Jeśli chcesz zmodyfikować szablon wiadomości administratora, wybierz zakładkę **Komunikat administratora**. Ta wiadomość jest tworzona automatycznie po kliknięciu przycisku **Wyślij przez e-mail** w oknie **Żądanie dostępu do zaszyfrowanych plików** i jest wysyłany do użytkownika po nadaniu mu uprawnień dostępu do zaszyfrowanych plików.

8. Zmodyfikuj szablony wiadomości.

Możesz użyć przycisku **Domyślny** oraz listy rozwijalnej **Zmienna**.

9. Zapisz swoje zmiany.

Szyfrowanie nośników wymiennych

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Kaspersky Endpoint Security obsługuje szyfrowanie plików w systemach plików FAT32 i NTFS. Jeśli dysk wymienny z nieobsługiwanym systemem plików jest podłączony do komputera, zadanie szyfrowania dla tego dysku wymiennego zakończy się błędem, a Kaspersky Endpoint Security przypisze do dysku wymiennego stan tylko do odczytu.

W celu ochrony danych na dyskach wymiennych możesz użyć następujących typów szyfrowania:

- Szyfrowanie całego dysku (FDE).
Szyfrowanie całego dysku wymiennego, w tym systemu plików.

Nie jest możliwy dostęp do zaszyfrowanych danych poza siecią korporacyjną. Dostęp do zaszyfrowanych danych w sieci korporacyjnej jest również niemożliwy, jeśli komputer nie jest podłączony do Kaspersky Security Center (na przykład, na komputerze gościa).

- Szyfrowanie na poziomie plików (FLE).

Szyfrowanie tylko plików na dysku wymiennym. System plików pozostaje niezmienny.

Szyfrowanie plików na dyskach wymiennych umożliwia dostęp do danych poza siecią korporacyjną za pomocą specjalnego trybu zwanego [trybem przenośnym](#).

Podczas szyfrowania Kaspersky Endpoint Security tworzy klucz główny. Kaspersky Endpoint Security zapisuje klucz główny w następujących repozytoriach:

- Kaspersky Security Center.

- Na komputerze użytkownika.

Klucz główny jest szyfrowany za pomocą tajnego klucza użytkownika.

- Na dysku wymiennym.

Klucz główny jest szyfrowany za pomocą klucza publicznego Kaspersky Security Center.

Po zakończeniu szyfrowania dane na dysku wymiennym mogą być dostępne w sieci korporacyjnej tak, jakbyś używał zwykłego niezasyfrowanego dysku wymiennego.

Uzyskiwanie dostępu do zaszyfrowanych danych

Gdy podłączony jest dysk wymienny z zaszyfrowanymi danymi, Kaspersky Endpoint Security wykonuje następujące czynności:

1. Sprawdza klucz główny w lokalnej pamięci na komputerze użytkownika.

Jeśli klucz główny zostanie znaleziony, użytkownik uzyskuje dostęp do danych na dysku wymiennym.

Jeśli klucz główny nie zostanie znaleziony, Kaspersky Endpoint Security wykonuje następujące działania:

- a. Wysyła zapytanie do Kaspersky Security Center.

Po otrzymaniu zapytania, Kaspersky Security Center wysyła odpowiedź zawierającą klucz główny.

- b. Kaspersky Endpoint Security zapisuje klucz główny w lokalnej pamięci na komputerze użytkownika do późniejszych operacji na zaszyfrowanym dysku wymiennym.

2. Odszyfrowuje dane.

Specjalne funkcje szyfrowania dysku wymiennego

Szyfrowanie dysków wymiennych ma następujące funkcje specjalne:

- Zasada z predefiniowanymi ustawieniami szyfrowania dysku wymiennego zostanie utworzona dla określonej grupy zarządzanych komputerów. Dlatego też, wynik stosowania profilu Kaspersky Security Center, skonfigurowanego dla szyfrowania/deszyfrowania dysków wymiennych zależy od komputera, do którego podłączony jest dysk wymienny.

- Kaspersky Endpoint Security nie szyfruje/deszyfruje plików tylko do odczytu, które są przechowywane na nośnikach wymiennych.
- Następujące typy urządzeń są obsługiwane jako dyski wymienne:
 - Nośniki danych podłączone poprzez magistralę USB
 - Dyski twarde podłączone poprzez magistrale USB i FireWire
 - Dyski SSD podłączone poprzez magistrale USB i FireWire

Uruchamianie szyfrowania nośników wymiennych

Możesz użyć zasady do odszyfrowania dysku wymiennego. Dla określonej grupy administracyjnej generowana jest zasada ze zdefiniowanymi ustawieniami szyfrowania dysku wymiennego. Dlatego też wynik deszyfrowania danych na dyskach wymiennych zależy od komputera, do którego podłączony został dysk wymienny.

Kaspersky Endpoint Security obsługuje szyfrowanie w systemach plików FAT32 i NTFS. Jeśli dysk wymienny z nieobsługiwanym systemem plików jest podłączony do komputera, szyfrowanie tego dysku wymiennego zakończy się błędem, a Kaspersky Endpoint Security przypisze do dysku wymiennego dostęp tylko do odczytu.

W celu zaszyfrowania dysków wymiennych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
6. Z listy rozwijalnej **Tryb szyfrowania** wybierz domyślne działanie, które Kaspersky Endpoint Security ma wykonać na dyskach wymiennych:
 - **Zaszyfruj cały dysk wymienny** (FDE). Kaspersky Endpoint Security zaszyfruje zawartość dysku wymiennego sektor po sektorze. W rezultacie aplikacja zaszyfruje nie tylko pliki przechowywane na dysku wymiennym, ale także jego systemy plików, w tym nazwy plików i struktury folderów na dysku wymiennym.
 - **Zaszyfruj wszystkie pliki** (FLE). Kaspersky Endpoint Security szyfruje wszystkie pliki, które są przechowywane na dyskach wymiennych. Aplikacja nie szyfruje systemów plików dysków wymiennych, łącznie z nazwami plików i strukturami folderów.
 - **Zaszyfruj tylko nowe pliki** (FLE). Kaspersky Endpoint Security szyfruje tylko te pliki, które zostały dodane do dysków wymiennych lub które były przechowywane na dyskach wymiennych i zostały zmodyfikowane po ostatnim zastosowaniu profilu Kaspersky Security Center.

Kaspersky Endpoint Security nie szyfruje dysku wymiennego, który został już zaszyfrowany.

7. Jeśli chcesz [użyć trybu przenośnego](#) dla szyfrowania dysków wymiennych, zaznacz pole **Tryb przenośny**.

Tryb przenośny to tryb szyfrowania plików (FLE) na dyskach wymiennych, które oferują możliwość dostępu do danych poza siecią korporacyjną. Tryb przenośny umożliwia także pracę z zaszyfrowanymi danymi na komputerach bez zainstalowanego programu Kaspersky Endpoint Security.

8. Jeśli chcesz zaszyfrować nowy dysk wymienny, zalecane jest zaznaczenie pola **Zaszyfruj tylko używaną przestrzeń dyskową**. Jeśli pole jest odznaczone, Kaspersky Endpoint Security zaszyfruje wszystkie pliki, w tym pozostałe fragmenty usuniętych lub zmodyfikowanych plików.

9. Jeśli chcesz skonfigurować szyfrowanie dla pojedynczych dysków wymiennych, [zdefiniuj reguły szyfrowania](#).

10. Jeśli chcesz użyć szyfrowania całego dysku dla dysków wymiennych w trybie offline, zaznacz pole **Zezwól na szyfrowanie dysków wymiennych w trybie offline**.

Tryb szyfrowania offline to szyfrowanie dysków wymiennych (FDE), gdy nie ma połączenia z Kaspersky Security Center. Podczas szyfrowania Kaspersky Endpoint Security zapisuje główny klucz tylko na komputerze użytkownika. Kaspersky Endpoint Security wyśle główny klucz do Kaspersky Security Center podczas następnej synchronizacji.

Jeśli komputer, na którym zapisany jest główny klucz, jest uszkodzony, a dane nie są wysyłane do Kaspersky Security Center, nie jest możliwe uzyskanie dostępu do dysku wymiennego.

Jeśli pole **Zezwól na szyfrowanie dysków wymiennych w trybie offline** jest odznaczone i nie ma połączenia z Kaspersky Security Center, szyfrowanie dysku wymiennego nie jest możliwe.

11. Zapisz swoje zmiany.

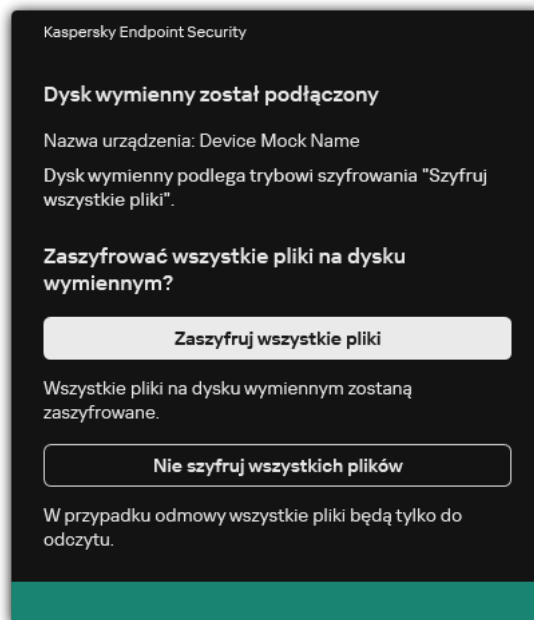
Po zastosowaniu profilu, gdy użytkownik podłącza dysk wymienny lub jeśli dysk wymienny jest już podłączony, Kaspersky Endpoint Security zapyta użytkownika o potwierdzenie wykonania operacji szyfrowania (patrz rysunek poniżej).

Aplikacja umożliwia wykonywanie następujących działań:

- Jeśli użytkownik potwierdzi żądanie szyfrowania, Kaspersky Endpoint Security zaszyfruje dane.
- Jeśli użytkownik odrzuci żądanie szyfrowania, Kaspersky Endpoint Security pozostawi dane niezmienione i przypisze dla tego dysku wymiennego dostęp tylko do odczytu.
- Jeśli użytkownik nie odpowie na żądanie szyfrowania, Kaspersky Endpoint Security pozostawi dane niezmienione i przypisze dla tego dysku wymiennego dostęp tylko do odczytu. Aplikacja ponownie wyświetli monit o potwierdzenie przy jednoczesnym zastosowaniu zasady lub następnym razem, gdy ten dysk wymienny zostanie podłączony.

Jeśli użytkownik zainicjuje bezpieczne usuwanie dysku wymiennego w trakcie szyfrowania danych, Kaspersky Endpoint Security przerwie proces szyfrowania i pozwoli na usunięcie dysku wymiennego przed zakończeniem procesu szyfrowania. Szyfrowanie danych będzie kontynuowane następnym razem, gdy dysk wymienny zostanie podłączony do tego komputera.

Jeśli szyfrowanie nośnika wymiennego nie powiodło się, przejrzyj raport **Szyfrowanie danych** w interfejsie Kaspersky Endpoint Security. Dostęp do plików może być zablokowany przez inną aplikację. W tym przypadku spróbuj odłączyć nośnik wymienny od komputera i podłączyć go ponownie.



Żądanie szyfrowania dysku wymiennego

Dodawanie reguły szyfrowania dla nośników wymiennych

W celu dodania reguły szyfrowania dla dysków wymiennych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
6. Kliknij przycisk **Dodaj** i z otwartej listy rozwijalnej wybierz jeden z następujących elementów:
 - Jeśli chcesz dodać regułę szyfrowania dla nośników wymiennych, które znajdują się na liście zaufanych urządzeń komponentu Kontrola urządzeń, wybierz **Z listy zaufanych urządzeń określonej w tej zasadzie**.
 - Jeśli chcesz dodać regułę szyfrowania dla nośników wymiennych, które znajdują się na liście Kaspersky Security Center, wybierz **Z listy urządzeń Kaspersky Security Center**.
7. Z listy rozwijalnej **Tryb szyfrowania dla wybranych urządzeń** wybierz akcję, jaka zostanie wykonana przez Kaspersky Endpoint Security na plikach przechowywanych na wybranych dyskach wymiennych.
8. Zaznacz pole **Tryb przenośny**, jeśli chcesz, aby przed szyfrowaniem program Kaspersky Endpoint Security przygotował dyski wymienne, umożliwiając użycie w trybie przenośnym przechowywanych na nich zaszyfrowanych plików.

Tryb przenośny umożliwia użycie zaszyfrowanych plików, przechowywanych na dyskach wymiennych podłączonych do komputerów [bez funkcji szyfrowania](#).

9. Jeśli chcesz, aby Kaspersky Endpoint Security szyfrował tylko te sektory dysku, które są zajęte przez pliki, zaznacz pole **Zaszyfruj tylko używaną przestrzeń dyskową**.

Jeśli stosujesz szyfrowanie na dysku, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku. Zapewni to ochronę wszystkich danych, także tych usuniętych, gdyż mogą zawierać informacje, które można odzyskać. Użycie funkcji **Zaszyfruj tylko używaną przestrzeń dyskową** jest zalecane w przypadku nowych dysków, które nie były wcześniej używane.

Jeśli urządzenie zostało wcześniej zaszyfrowane przy użyciu funkcji **Zaszyfruj tylko używaną przestrzeń dyskową**, po zastosowaniu profilu w trybie **Zaszyfruj cały dysk wymienny**, sektory, które nie są zajęte przez pliki, będą wciąż niezaszyfrowane.

10. Z listy rozwijalnej **Działania dla urządzeń wybranych wcześniej** wybierz akcję wykonywaną przez Kaspersky Endpoint Security zgodnie z regułami szyfrowania, wcześniej zdefiniowanymi dla dysków wymiennych:

- Jeśli chcesz, aby wcześniej utworzona reguła szyfrowania dla nośnika wymiennego pozostała niezmieniona, wybierz **Pomiń**.
- Jeśli chcesz, aby wcześniej utworzona reguła szyfrowania dla nośnika wymiennego została zastąpiona przez nową regułę, wybierz **Aktualizuj**.

11. Zapisz swoje zmiany.

Dodane reguły szyfrowania dysków wymiennych zostaną zastosowane do dysków wymiennych podłączonych do dowolnych komputerów w organizacji.

Eksportowanie i importowanie listy reguł szyfrowania dla nośników wymiennych

Możesz wyeksportować listę reguł szyfrowania nośników wymiennych do pliku XML. Następnie możesz zmodyfikować plik, na przykład, aby zwiększyć liczbę reguł tego samego typu nośników wymiennych. Możesz także użyć funkcji eksportowania/importowania do utworzenia kopii zapasowej listy reguł lub przeniesienia reguł na inny serwer.

[Eksportowanie i importowanie listy reguł szyfrowania nośników wymiennych w Konsoli administracyjnej \(MMC\)](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
6. W celu wyeksportowania listy reguł szyfrowania dla nośników wymiennych:
 - a. Wybierz reguły, które chcesz zmienić. Aby wybrać kilka portów, użyj klawisza **CTRL** lub **SHIFT**.
Jeśli nie wybrałeś żadnej reguły, Kaspersky Endpoint Security wyeksportuje wszystkie reguły.
 - b. Kliknij odnośnik **Eksportuj**.
 - c. W otwartym oknie określ nazwę pliku XML, do którego chcesz wyeksportować listę reguł, i wybierz folder, w którym chcesz zapisać ten plik.
 - d. Kliknij przycisk **Zapisz**.
Kaspersky Endpoint Security eksportuje listę reguł do pliku XML.
7. W celu zaimportowania listy reguł szyfrowania dla nośników wymiennych:
 - a. Kliknij odnośnik **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
 - b. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.

[Eksportowanie i importowanie listy reguł szyfrowania nośników wymiennych w Web Console](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasadę Kaspersky Endpoint Security dla komputerów, na których chcesz wyeksportować lub zaimportować listę reguł szyfrowania nośników wymiennych.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
5. W sekcji **Reguły szyfrowania dla wybranych urządzeń** kliknij odnośnik **Reguły szyfrowania**.
Spowoduje to otwarcie listy reguł szyfrowania dla nośników wymiennych.
6. W celu wyeksportowania listy reguł szyfrowania dla nośników wymiennych:
 - a. Wybierz reguły, które chcesz zmienić.
 - b. Kliknij przycisk **Eksportuj**.
 - c. Potwierdź chęć wyeksportowania tylko wybranych reguł lub wyeksportuj całą listę.
 - d. Kliknij przycisk **Eksportuj**.
Kaspersky Endpoint Security eksportuje listę reguł do pliku XML w domyślnym folderze do pobrania.
7. W celu zaimportowania listy reguł:
 - a. Kliknij odnośnik **Importuj**.
W oknie, które zostanie otwarte, wybierz plik XML, z którego chcesz zaimportować listę reguł.
 - b. Kliknij przycisk **Otwórz**.
Jeśli komputer ma już listę reguł, Kaspersky Endpoint Security wyświetli monit o usunięcie istniejącej listy lub dodanie do niej nowych wpisów z pliku XML.
8. Zapisz swoje zmiany.

Tryb przenośny dla uzyskiwania dostępu do zaszyfrowanych plików na dyskach wymiennych

Tryb przenośny to tryb szyfrowania plików (FLE) na dyskach wymiennych, które oferują możliwość dostępu do danych poza siecią korporacyjną. Tryb przenośny umożliwia także pracę z zaszyfrowanymi danymi na komputerach bez zainstalowanego programu Kaspersky Endpoint Security.

Tryb przenośny jest wygodny w użyciu w następujących przypadkach:

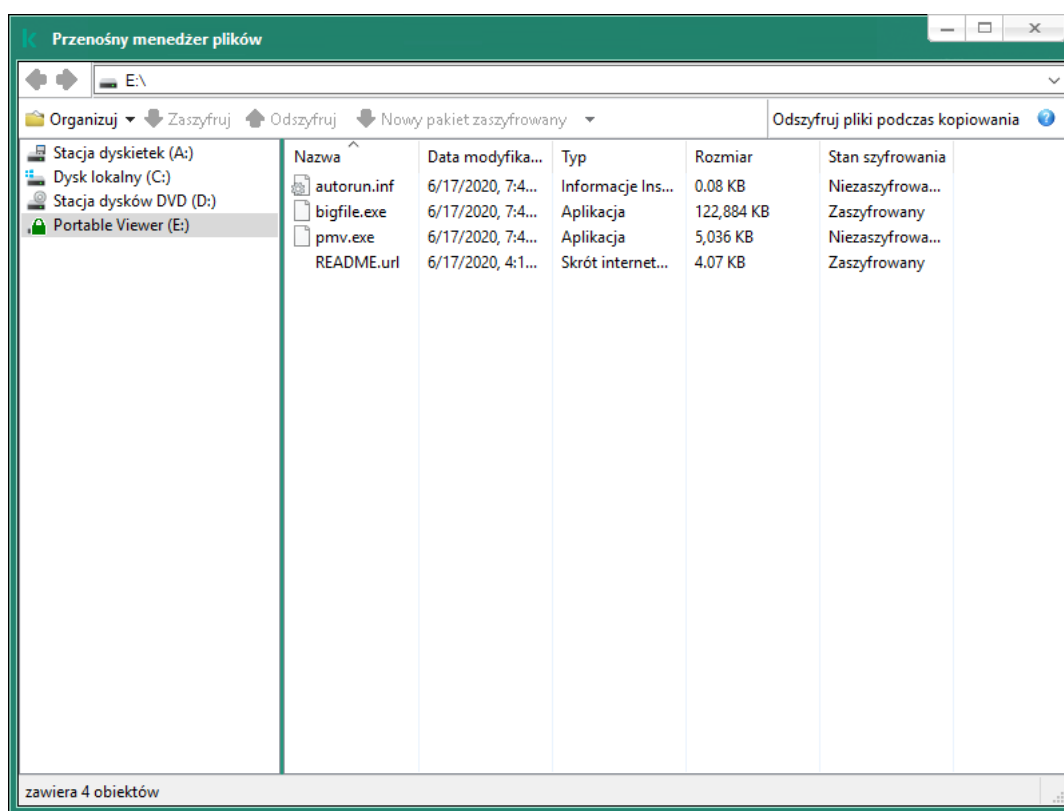
- Nie ma połączenia między komputerem a Serwerem administracyjnym Kaspersky Security Center.
- Infrastruktura zmieniła się wraz ze zmianą Serwera administracyjnego Kaspersky Security Center.
- Kaspersky Endpoint Security nie jest zainstalowany na komputerze.

Przenośny menedżer plików

Aby pracować w trybie przenośnym, Kaspersky Endpoint Security instaluje specjalny moduł szyfrowania o nazwie *Przenośny menedżer plików* na dysku wymiennym. Przenośny menedżer plików zapewnia interfejs do pracy z zaszyfrowanymi danymi, jeśli Kaspersky Endpoint Security nie jest zainstalowany na komputerze (patrz rysunek poniżej). Jeśli na Twoim komputerze jest zainstalowany Kaspersky Endpoint Security, możesz pracować z zaszyfrowanymi dyskami wymiennymi przy użyciu zwykłego menedżera plików (na przykład Eksploratora).

Przenośny menedżer plików przechowuje klucz do szyfrowania plików na dysku wymiennym. Klucz jest szyfrowany hasłem użytkownika. Użytkownik ustawia hasło przed zaszyfrowaniem plików na dysku wymiennym.

Przenośny menedżer plików uruchamia się automatycznie, gdy dysk wymienny jest podłączony do komputera, na którym nie jest zainstalowany Kaspersky Endpoint Security. Jeśli automatyczne uruchamianie aplikacji jest wyłączone na komputerze, ręcznie uruchom Przenośny menedżer plików. Aby to zrobić, uruchom plik o nazwie *pmv.exe*, który jest przechowywany na dysku wymiennym.



Przenośny menedżer plików

Obsługa trybu przenośnego do pracy z zaszyfrowanymi plikami

[Jak włączyć obsługę trybu przenośnego podczas pracy z zaszyfrowanymi plikami na dyskach wymiennych w Konsoli administracyjnej \(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
6. Z listy rozwijanej **Tryb szyfrowania dla wybranych urządzeń** wybierz **Zaszyfruj wszystkie pliki** lub **Zaszyfruj tylko nowe pliki**.

Tryb przenośny jest dostępny tylko z Szyfrowaniem plików (FLE). Nie można włączyć obsługi trybu przenośnego dla Szyfrowania całego dysku (FDE).

7. Zaznacz pole **Tryb przenośny**.
8. Jeśli to konieczne, [dodaj reguły szyfrowania dla poszczególnych dysków wymiennych](#).
9. Zapisz swoje zmiany.
10. Po zastosowaniu zasady, podłącz dysk wymienny do komputera.
11. Potwierdź operację szyfrowania nośnika wymiennego.
Zostanie otwarte okno, w którym można utworzyć hasło dla Przenośnego Menedżera plików.
12. Określ hasło, które spełnia wymagania co do siły, i potwierdź je.
13. Zapisz swoje zmiany.

Kaspersky Endpoint Security szyfruje pliki na dysku wymiennym. Przenośny menedżer plików używany do pracy z zaszyfrowanymi plikami także zostanie dodany na nośniku wymiennym. Jeśli na dysku wymiennym znajdują się już zaszyfrowane pliki, Kaspersky Endpoint Security zaszyfruje je ponownie przy użyciu własnego klucza. Umożliwia to użytkownikowi dostęp do wszystkich plików na dysku wymiennym w trybie przenośnym.

[Jak włączyć obsługę trybu przenośnego podczas pracy z zaszyfrowanymi plikami na dyskach wymiennych w konsoli Web Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security dla komputerów, na których chcesz włączyć obsługę trybu przenośnego.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
5. W sekcji **Zarządzanie szyfrowaniem** wybierz **Zaszyfruj wszystkie pliki** lub **Zaszyfruj tylko nowe pliki**.

Tryb przenośny jest dostępny tylko z Szyfrowaniem plików (FLE). Nie można włączyć obsługi trybu przenośnego dla Szyfrowania całego dysku (FDE).

6. Zaznacz pole **Tryb przenośny**.
7. Jeśli to konieczne, [dodaj reguły szyfrowania dla poszczególnych dysków wymiennych](#).
8. Zapisz swoje zmiany.
9. Po zastosowaniu zasady, podłącz dysk wymienny do komputera.
10. Potwierdź operację szyfrowania nośnika wymiennego.
Zostanie otwarte okno, w którym można utworzyć hasło dla Przenośnego Menedżera plików.
11. Określ hasło, które spełnia wymagania co do siły, i potwierdź je.
12. Zapisz swoje zmiany.

Kaspersky Endpoint Security szyfruje pliki na dysku wymiennym. Przenośny menedżer plików używany do pracy z zaszyfrowanymi plikami także zostanie dodany na nośniku wymiennym. Jeśli na dysku wymiennym znajdują się już zaszyfrowane pliki, Kaspersky Endpoint Security zaszyfruje je ponownie przy użyciu własnego klucza. Umożliwia to użytkownikowi dostęp do wszystkich plików na dysku wymiennym w trybie przenośnym.

Uzyskiwanie dostępu do zaszyfrowanych plików na dysku wymiennym

Po zaszyfrowaniu plików na dysku wymiennym z obsługą trybu przenośnego dostępne są następujące metody uzyskania dostępu do plików:

- Jeśli Kaspersky Endpoint Security nie jest zainstalowany na komputerze, Przenośny menedżer plików poprosi o podanie hasła. Konieczne będzie wprowadzenie hasła przy każdym ponownym uruchomieniu komputera lub ponownym podłączeniu dysku wymiennego.
- Jeśli komputer znajduje się poza siecią korporacyjną, a na nim jest zainstalowany program Kaspersky Endpoint Security, aplikacja poprosi o podanie hasła lub wyśle administratorowi żądanie dostępu do plików. Po uzyskaniu dostępu do plików na dysku wymiennym Kaspersky Endpoint Security zapisze tajny klucz w pamięci kluczy komputera. Umożliwi to dostęp do plików w przyszłości bez konieczności wprowadzania hasła lub pytania administratora.

- Jeśli komputer znajduje się w sieci korporacyjnej, a na nim jest zainstalowany program Kaspersky Endpoint Security, uzyskasz dostęp do urządzenia bez podawania hasła. Kaspersky Endpoint Security otrzyma tajny klucz z Serwera administracyjnego Kaspersky Security Center, z którym komputer jest połączony.

Odzyskiwanie hasła do pracy w trybie przenośnym

Jeśli zapomniałeś hasła do pracy w trybie przenośnym, musisz podłączyć dysk wymienny do komputera z programem Kaspersky Endpoint Security zainstalowanym w sieci korporacyjnej. Uzyskasz dostęp do plików, ponieważ tajny klucz jest przechowywany w pamięci kluczy komputera lub na Serwerze administracyjnym. Odszyfruj i ponownie zaszyfruj pliki za pomocą nowego hasła.

Funkcje trybu przenośnego podczas podłączania dysku wymiennego do komputera z innej sieci

Jeśli komputer znajduje się poza siecią korporacyjną, a na nim jest zainstalowany program Kaspersky Endpoint Security, uzyskasz dostęp do plików w następujące sposoby:

- **Dostęp oparty na hasle**

Po wprowadzeniu hasła, możliwe będzie przeglądanie, modyfikowanie i zapisywanie plików na dysku wymiennym (*przezroczysty dostęp*). Kaspersky Endpoint Security może ustawić prawo dostępu tylko do odczytu dla dysku wymiennego, jeśli w ustawieniach zasady skonfigurowane są następujące parametry szyfrowania dysków wymiennych:

- Obsługa trybu przenośnego jest wyłączona.
- Tryb **Zaszyfruj wszystkie pliki** lub **Zaszyfruj tylko nowe pliki** został wybrany.

We wszystkich pozostałych przypadkach uzyskasz pełny dostęp do dysku wymiennego (uprawnienie do odczytu/zapisu). Będziesz mógł dodawać i usuwać pliki.

Możesz zmienić uprawnienia dostępu do dysku wymiennego nawet wtedy, gdy dysk wymienny jest podłączony do komputera. Jeśli uprawnienia dostępu do dysku wymiennego zostały zmienione, Kaspersky Endpoint Security zablokuje dostęp do plików i ponownie wyświetli pytanie o podanie hasła.

Po wprowadzeniu hasła nie możesz zastosować ustawień zasady szyfrowania do dysku wymiennego. W tym przypadku niemożliwe jest odszyfrowanie lub ponowne zaszyfrowanie plików na dysku wymiennym.

- **Zapytaj administratora o dostęp do plików**

Jeśli zapomniałeś hasła do pracy w trybie przenośnym, poproś administratora o dostęp do plików. Aby uzyskać dostęp do plików, użytkownik powinien wysłać do administratora plik żądania dostępu (plik z rozszerzeniem KESDC). Na przykład, użytkownik może wysłać plik żądania dostępu za pośrednictwem poczty elektronicznej. Administrator wyśle zaszyfrowany plik dostępu do danych (plik z rozszerzeniem KESDR).

Po zakończeniu procedury odzyskiwania hasła Żądanie-Odpowiedź, uzyskasz przezroczysty dostęp do plików na dysku wymiennym, a także pełny dostęp do dysku wymiennego (uprawnienie do odczytu/zapisu).

Na przykład, możesz zastosować zasadę szyfrowania dysku wymiennego i odszyfrować pliki. Po odzyskaniu hasła lub gdy zasada zostanie zaktualizowana, Kaspersky Endpoint Security wyświetli pytanie o potwierdzenie wprowadzenia zmian.

[Jak uzyskać plik dostępu do zaszyfrowanych danych w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
4. Na zakładce **Urządzenia** wybierz komputer użytkownika, który żąda dostępu do zaszyfrowanych danych, i kliknij go prawym przyciskiem myszy.
5. Z menu kontekstowego wybierz **Przydziel dostęp w trybie offline**.
6. W otwartym oknie wybierz zakładkę **Szyfrowanie danych**.
7. Na zakładce **Szyfrowanie danych** kliknij przycisk **Przeglądaj**.
8. W oknie wyboru pliku dostępu do żądania określ ścieżkę do pliku otrzymanego od użytkownika.

Zobaczysz informacje o żądaniu użytkownika. Kaspersky Security Center wygeneruje plik klucza. Wyślij do użytkownika wygenerowany plik klucza dostępu do zaszyfrowanych danych. Lub zapisz plik dostępu i użyj dowolnej dostępnej metody, aby przenieść plik.

[Jak uzyskać plik dostępu do zaszyfrowanych danych w konsoli Web Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Zaznacz pole wyboru obok nazwy komputera, do którego danych chcesz przywrócić dostęp.
3. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.
4. Wybierz sekcję **Szyfrowanie danych**.
5. Kliknij przycisk **Wybierz plik** i wybierz plik żądania dostępu otrzymany od użytkownika (plik z rozszerzeniem KESDC).
Konsola Web Console wyświetli informacje o żądaniu. Obejmuje to nazwę komputera, na którym użytkownik żąda dostępu do pliku.
6. Kliknij przycisk **Zapisz klucz** i wybierz folder, aby zapisać plik klucza dostępu do zaszyfrowanych danych (plik z rozszerzeniem KESDR).

W rezultacie będziesz mógł uzyskać klucz dostępu do zaszyfrowanych danych, który będziesz musiał przekazać użytkownikowi.

Deszyfrowanie nośników wymiennych

Możesz użyć zasady do odszyfrowania dysku wymiennego. Dla określonej grupy administracyjnej generowana jest zasada ze zdefiniowanymi ustawieniami szyfrowania dysku wymiennego. Dlatego też wynik deszyfrowania danych na dyskach wymiennych zależy od komputera, do którego podłączony został dysk wymienny.

W celu odszyfrowania dysków wymiennych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasad wybierz **Szyfrowanie danych** → **Szyfrowanie dysków wymiennych**.
6. Jeśli chcesz odszyfrować wszystkie zaszyfrowane pliki przechowywane na dyskach wymiennych, z listy rozwijalnej **Tryb szyfrowania** wybierz **Odszyfruj cały dysk wymienny**.
7. Aby odszyfrować dane przechowywane na pojedynczych dyskach wymiennych, zmodyfikuj reguły szyfrowania dla dysków wymiennych, których dane chcesz odszyfrować. W tym celu:
 - a. Na liście nośników wymiennych, dla których skonfigurowano reguły szyfrowania, wybierz wpis odpowiadający żadanemu nośnikowi wymiennemu.
 - b. Kliknij przycisk **Określ regułę**, aby zmodyfikować regułę szyfrowania dla wybranego dysku wymiennego.
 - c. W menu kontekstowym przycisku **Określ regułę** kliknij **Odszyfruj cały dysk wymienny**.
8. Zapisz swoje zmiany.

W rezultacie, jeśli użytkownik podłącza dysk wymienny lub jest już podłączony, Kaspersky Endpoint Security odszyfrowuje dysk wymienny. Aplikacja ostrzega użytkownika, że proces deszyfrowania może zająć trochę czasu. Jeśli użytkownik zainicjuje bezpieczne usunięcie dysku wymiennego w trakcie deszyfrowania danych, Kaspersky Endpoint Security przerwie proces deszyfrowania i pozwoli na usunięcie dysku wymiennego przed zakończeniem procesu deszyfrowania. Deszyfrowanie danych będzie kontynuowane następnym razem, gdy dysk wymienny zostanie podłączony do komputera.

Jeśli deszyfrowanie nośnika wymiennego nie powiodło się, przejrzyj raport **Szyfrowanie danych** w interfejsie Kaspersky Endpoint Security. Dostęp do plików może być zablokowany przez inną aplikację. W tym przypadku spróbuj odłączyć nośnik wymienny od komputera i podłączyć go ponownie.

Przeglądanie informacji szczegółowych dotyczących szyfrowania danych

Podczas wykonywania procesu szyfrowania lub deszyfrowania program Kaspersky Endpoint Security wysyła do Kaspersky Security Center informacje o stanie parametrów szyfrowania zastosowanych na komputerach klienckich.

Możliwe są następujące wartości stanów szyfrowania:

- *Profil szyfrowania nie został zdefiniowany.* Profil szyfrowania Kaspersky Security Center nie został zdefiniowany dla komputera.
- *Stosowanie profilu.* Na komputerze przeprowadzane jest szyfrowanie i / lub deszyfrowanie danych.

- *Błąd.* Podczas procesu szyfrowania i / lub deszyfrowania danych wystąpił błąd.
- *Wymagane jest ponowne uruchomienie.* System operacyjny musi zostać uruchomiony ponownie w celu rozpoczęcia lub zakończenia szyfrowania lub deszyfrowania danych.
- *Zgodny z profilem.* Szyfrowanie danych na komputerze zostało wykonane przy użyciu ustawień szyfrowania określonych w profilu Kaspersky Security Center, zastosowanym na komputerze.
- *Anulowane przez użytkownika.* Użytkownik odmówił potwierdzenia działania szyfrowania plików na nośniku wymiennym.

Sprawdzanie stanu szyfrowania

W celu wyświetlenia stanu szyfrowania danych komputera:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Urządzenia**.
Zakładka **Urządzenia** w obszarze roboczym wyświetla właściwości komputerów w wybranej grupie administracyjnej.
4. Na zakładce **Urządzenia** w obszarze roboczym przesunij suwak w prawą stronę, do samego końca.
5. Jeśli kolumna **Stan szyfrowania** nie jest wyświetlana:
 - a. Kliknij prawym przyciskiem myszy, aby otworzyć menu kontekstowe nagłówka tabeli.
 - b. W menu kontekstowym, z listy rozwijalnej **Widok** wybierz **Dodaj/Usuń kolumny**.
 - c. W otwartym oknie zaznacz pole **Stan szyfrowania**.
6. Kliknij **OK**.

Kolumna **Stan szyfrowania** wyświetla stan szyfrowania danych na komputerach w wybranej grupie administracyjnej. Ten stan jest tworzony w oparciu o informacje o szyfrowaniu plików na dyskach lokalnych komputera oraz o szyfrowaniu całego dysku.

Przeglądanie statystyk szyfrowania dotyczących pulpitów nawigacyjnych Kaspersky Security Center

W celu przejrzania statystyk szyfrowania dotyczących pulpitów nawigacyjnych Kaspersky Security Center:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie konsoli wybierz węzeł **Serwer administracyjny – <Nazwa komputera>**.
3. W obszarze roboczym po prawej stronie drzewa Konsoli administracyjnej, wybierz zakładkę **Statystyki**.

4. Utwórz nową stronę z panelami szczegółów zawierającą statystyki szyfrowania danych. W tym celu:

a. Na zakładce **Statystyki** kliknij przycisk **Dostosuj widok**.

Zostanie otwarte okno **Właściwości: Statystyki**.

b. W oknie **Właściwości: Statystyki** kliknij **Dodaj**.

Zostanie otwarte okno **Właściwości: Nowa strona**.

c. W sekcji **Ogólne** okna **Właściwości: Nowa strona** wpisz nazwę strony.

d. W sekcji **Panele informacyjne** kliknij przycisk **Dodaj**.

Zostanie otwarte okno **Nowy panel informacyjny**.

e. W oknie **Nowy panel informacyjny** grupy **Stan ochrony** wybierz element **Szyfrowanie urządzeń**.

f. Kliknij **OK**.

Zostanie otwarte okno **Właściwości: Kontrola szyfrowania**.

g. Jeśli to konieczne, zmodyfikuj ustawienia panelu szczegółów. Aby to zrobić, skorzystaj z sekcji **Widok i Urządzenia** okna **Właściwości: Szyfrowanie urządzeń**.

h. Kliknij **OK**.

i. Powtórz czynności z kroków d – h, wybierając element **Szyfrowanie dysków wymiennych** w sekcji **Stan ochrony** okna **Nowy panel informacyjny**.

Dodane panele szczegółów pojawią się na liście **Panele informacyjne** w oknie **Właściwości: Nowa strona**.

j. W oknie **Właściwości: Nowa strona** kliknij **OK**.

Nazwa strony z panelami szczegółów utworzona w poprzednich krokach pojawi się na liście **Strony** okna **Właściwości: Statystyki**.

k. W oknie **Właściwości: Statystyki** kliknij **Zamknij**.

5. Na zakładce **Statystyki** otwórz stronę utworzoną w poprzednich krokach instrukcji.

Pojawią się panele szczegółów wyświetlające stan szyfrowania komputerów i dysków wymiennych.

Przeglądanie błędów szyfrowania plików na lokalnych dyskach komputera

W celu wyświetlenia błędów szyfrowania plików na lokalnych dyskach komputera:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.

2. W drzewie Konsoli administracyjnej, w folderze **Zarządzane urządzenia** otwórz folder z nazwą grupy administracyjnej zawierającej komputer kliencki, którego listę błędów szyfrowania plików chcesz przejrzeć.

3. W obszarze roboczym wybierz zakładkę **Urządzenia**.

4. Na zakładce **Urządzenia** wybierz nazwę komputera na liście i kliknij ją prawym przyciskiem myszy w celu otwarcia menu kontekstowego.

5. Z menu kontekstowego komputera wybierz element **Właściwości**. W oknie **Właściwości: <nazwa komputera>** wybierz sekcję **Ochrona**.

6. W sekcji **Ochrona** okna **Właściwości: <nazwa komputera>** kliknij odnośnik **Wyświetl błędy szyfrowania danych**, aby otworzyć okno **Błędy szyfrowania danych**.

To okno wyświetla szczegółowe informacje dotyczące błędów szyfrowania plików na lokalnych dyskach komputera. Po naprawieniu błędu, Kaspersky Security Center usunie szczegóły dotyczące błędu z okna **Błędy szyfrowania danych**.

Przeglądanie raportu z szyfrowania danych

W celu wyświetlenia raportu z szyfrowania danych:

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W węźle **Serwer administracyjny** drzewa Konsoli administracyjnej wybierz zakładkę **Raporty**.
3. Kliknij przycisk **Nowy szablon raportu**.
Zostanie uruchomiony Kreator tworzenia nowego szablonu raportu.
4. Postępuj zgodnie z instrukcjami Kreatora szablonu raportu. W oknie **Wybieranie typu szablonu raportu**, w sekcji **Inne** wybierz jeden z następujących elementów:

- **Raport o stanie szyfrowania zarządzanych urządzeń.**
- **Raport o stanie szyfrowania urządzeń pamięci masowej.**
- **Raport o błędach podczas szyfrowania plików.**
- **Raport o zablokowanym dostępie do zaszyfrowanych plików.**

Po zakończeniu pracy Kreatora nowego szablonu raportu, nowy szablon raportu pojawi się w tabeli, na zakładce **Raporty**.

5. Wybierz szablon raportu, który został utworzony w poprzednich krokach instrukcji.
6. Z menu kontekstowego szablonu wybierz **Pokaż raport**.

Zostanie rozpoczęty proces tworzenia raportu. Raport zostanie wyświetlony w nowym oknie.

Praca z zaszyfrowanymi urządzeniami, gdy nie ma dostępu do nich

Uzyskiwanie dostępu do zaszyfrowanych urządzeń

Prośba o dostęp do zaszyfrowanych urządzeń może być konieczna w następujących przypadkach:

- Dysk twardy został zaszyfrowany na innym komputerze.
- Klucz szyfrowania dla urządzenia nie znajduje się na komputerze (na przykład, po pierwszej próbie dostępu do zaszyfrowanego nośnika wymiennego na komputerze), a komputer nie jest połączony z Kaspersky Security Center.

Jeśli użytkownik zastosuje klucz dostępu do zaszyfrowanego urządzenia, Kaspersky Endpoint Security zapisze klucz szyfrowania na komputerze użytkownika i zezwoli na dostęp do tego urządzenia po kolejnych próbach uzyskania dostępu nawet wtedy, gdy nie ma połączenia z Kaspersky Security Center.

Dostęp do zaszyfrowanych urządzeń można uzyskać w następujący sposób:

1. Użytkownik wykorzystuje interfejs aplikacji Kaspersky Endpoint Security do utworzenia pliku żądania dostępu z rozszerzeniem kesdc i wysyła go do administratora firmowej sieci LAN.
2. Administrator wykorzystuje Konsolę administracyjną Kaspersky Security Center do utworzenia pliku klucza dostępu z rozszerzeniem kesdr i wysyła go do użytkownika.
3. Użytkownik stosuje klucz dostępu.

Odzyskiwanie danych na zaszyfrowanych urządzeniach

Do pracy z zaszyfrowanymi urządzeniami użytkownik może wykorzystać [Narzędzie przywracania zaszyfrowanego urządzenia](#) (zwane dalej Narzędziem przywracania). Taka sytuacja może mieć miejsce w następujących przypadkach:

- Procedura wykorzystania klucza dostępu do uzyskania dostępu nie powiodła się.
- Moduły szyfrujące nie zostały zainstalowane na zaszyfrowanym urządzeniu.

Dane niezbędne do przywrócenia dostępu do zaszyfrowanych urządzeń przy użyciu Narzędzia przywracania znajdują się od jakiegoś czasu w pamięci komputera użytkownika w postaci niezaszyfrowanej. Aby zmniejszyć ryzyko nieautoryzowanego dostępu do tych danych, zalecane jest przywrócenie dostępu do zaszyfrowanych urządzeń na zaufanych komputerach.

Dane na zaszyfrowanych urządzeniach można odzyskać w następujący sposób:

1. Użytkownik wykorzystuje Narzędzie przywracania do utworzenia pliku żądania dostępu z rozszerzeniem fdertc i wysyła go do administratora firmowej sieci LAN.
2. Administrator wykorzystuje Konsolę administracyjną Kaspersky Security Center do utworzenia pliku klucza dostępu z rozszerzeniem fdertr i wysyła go do użytkownika.
3. Użytkownik stosuje klucz dostępu.

Aby przywrócić dane na zaszyfrowanych dyskach twardych, użytkownik może także określić dane uwierzytelniające konta Agenta autoryzacji w Narzędziu przywracania. Jeśli metadane konta Agenta autoryzacji zostały uszkodzone, użytkownik musi zakończyć procedurę przywracania przy użyciu pliku żądania dostępu.

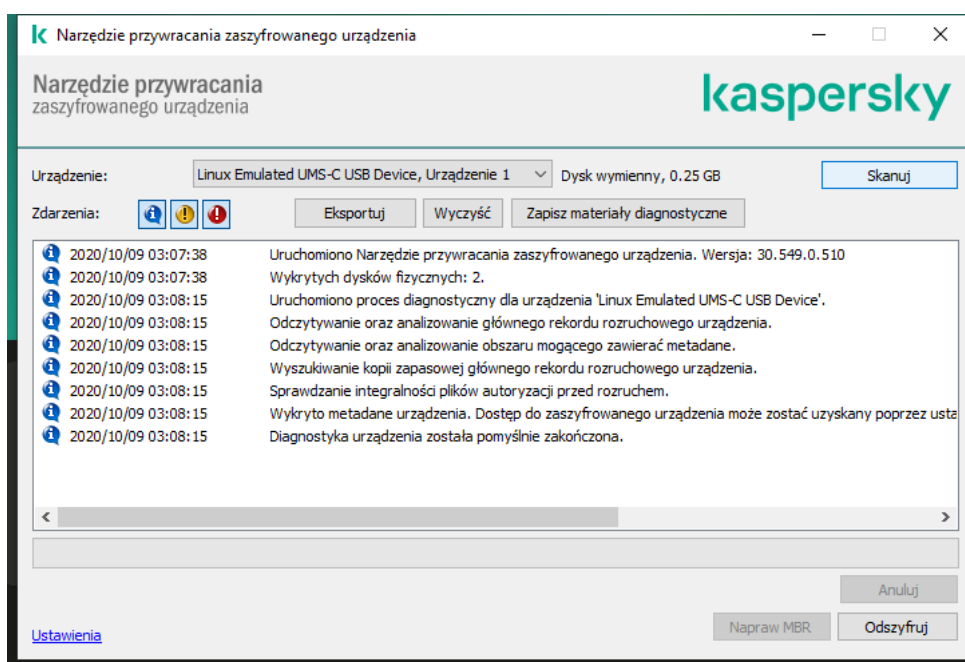
Przed przywróceniem danych na zaszyfrowanych urządzeniach zalecane jest anulowanie profilu Kaspersky Security Center lub wyłączenie szyfrowania w ustawieniach profilu Kaspersky Security Center na komputerze, na którym została wykonana procedura. Zapobiega to ponownemu zaszyfrowaniu urządzenia.

Odzyskiwanie danych za pomocą narzędzia przywracania FDERT

Jeśli dysk twardy ulegnie awarii, system plików może być uszkodzony. W takim przypadku dane chronione przez technologię Kaspersky Disk Encryption będą niedostępne. Możesz odszyfrować dane i skopiować je na nowy dysk.

Odzyskiwanie danych na dysku chronionym przez technologię Kaspersky Disk Encryption składa się z następujących kroków:

1. Utwórz autonomiczne narzędzie przywracania (patrz rysunek poniżej).
2. Podłącz dysk do komputera, na którym nie są zainstalowane komponenty szyfrujące Kaspersky Endpoint Security.
3. Uruchom narzędzie przywracania i zdiagnozuj dysk twardy.
4. Uzyskaj dostęp do danych na dysku. Aby to zrobić, wprowadź dane uwierzytelniające Agenta autoryzacji lub rozpocznij procedurę odzyskiwania (Żądanie-Odpowiedź).



Narzędzie przywracania FDERT

Tworzenie autonomicznego narzędzia przywracania

W celu utworzenia pliku wykonywalnego Narzędzia przywracania zaszyfrowanego urządzenia:

1. W oknie głównym aplikacji kliknij przycisk **Pomoc techniczna**.
2. W otwartym oknie kliknij przycisk **Przywróć zaszyfrowane urządzenie**.
Zostanie uruchomione Narzędzie do przywracania zaszyfrowanego urządzenia.
3. W oknie Narzędzia przywracania kliknij przycisk **Utwórz wersję autonomiczną Narzędzia przywracania**.
4. Zapisz autonomiczne narzędzie przywracania do pamięci komputera.

W rezultacie plik wykonywalny narzędzia przywracania (fdert.exe) zostanie zapisany w określonym folderze. Skopiuj narzędzie przywracania na komputer, na którym nie są zainstalowane komponenty szyfrujące Kaspersky Endpoint Security. Zapobiega to ponownemu zaszyfrowaniu dysku.

Dane niezbędne do przywrócenia dostępu do zaszyfrowanych urządzeń przy użyciu Narzędzia przywracania znajdują się od jakiegoś czasu w pamięci komputera użytkownika w postaci niezaszyfrowanej. Aby zmniejszyć ryzyko nieautoryzowanego dostępu do tych danych, zalecane jest przywrócenie dostępu do zaszyfrowanych urządzeń na zaufanych komputerach.

Odzyskiwanie danych na dysku twardym

W celu przywrócenia dostępu do zaszyfrowanego urządzenia przy użyciu Narzędzia przywracania zaszyfrowanego urządzenia:

1. Uruchom plik o nazwie fdert.exe, który jest plikiem wykonywalnym narzędzia przywracania. Ten plik jest tworzony przez Kaspersky Endpoint Security.
2. W oknie Narzędzie przywracające wybierz zaszyfrowane urządzenie, do którego dostęp chcesz odzyskać.
3. Kliknij przycisk **Skanowanie**, aby umożliwić narzędziu określenie akcji, jakie powinny zostać podjęte na urządzeniu: czy powinno zostać odblokowane, czy odszyfrowane.

Jeśli komputer posiada dostęp do funkcji szyfrowania programu Kaspersky Endpoint Security, Narzędzie przywracania wyświetli okno z pytaniem o odblokowanie urządzenia. Mimo, że odblokowanie urządzenia nie odszyfrowuje go, w wyniku odblokowania urządzenie staje się bezpośrednio dostępne. Jeśli komputer nie posiada dostępu do funkcji szyfrowania programu Kaspersky Endpoint Security, Narzędzie przywracania wyświetli okno z pytaniem o odszyfrowanie urządzenia.

4. Jeśli chcesz zaimportować informacje diagnostyczne, kliknij przycisk **Zapisz materiały diagnostyczne**. Narzędzie zapisze archiwum z plikami zawierającymi informacje diagnostyczne.
5. Kliknij przycisk **Napraw MBR**, jeśli diagnostyka zaszyfrowanego systemowego dysku twardego zwróciła wiadomość o problemach związanych z głównym rekordem rozruchowym (MBR) urządzenia.
Naprawienie głównego rekordu rozruchowego urządzenia może przyspieszyć proces uzyskiwania informacji niezbędnych do odblokowywania lub deszyfrowania urządzenia.
6. W zależności od wyników diagnostyki kliknij przycisk **Odblokuj** lub **Odszyfruj**.
7. Jeśli chcesz przywrócić dane przy użyciu konta Agenta autoryzacji, wybierz opcję **Użyj ustawień konta Agenta autoryzacji** i wprowadź dane uwierzytelniające Agenta autoryzacji.
Ta metoda jest możliwa tylko podczas przywracania danych na systemowym dysku twardym. Jeśli systemowy dysk twardy został uszkodzony, a dane konta Agenta autoryzacji zostały utracone, przywrócenie danych na zaszyfrowanym urządzeniu będzie możliwe po uzyskaniu klucza dostępu od administratora firmowej sieci LAN.
8. Jeśli chcesz rozpocząć procedurę odzyskiwania, wykonaj następujące czynności:
 - a. Wybierz opcję **Określ ręcznie klucz dostępu do urządzenia**.
 - b. Kliknij przycisk **Pobierz klucz dostępu** i zapisz plik żądania dostępu do pamięci komputera (plik z rozszerzeniem FDERTC).
 - c. Wyślij plik żądania dostępu do administratora firmowej sieci LAN.

Nie zamykaj okna **Pobierz klucz dostępu do urządzenia**, dopóki nie otrzymasz klucza dostępu. Jeśli to okno zostanie otwarte ponownie, nie będziesz mógł zastosować klucza dostępu, który wcześniej został utworzony przez administratora.

d. Pobierz i zapisz plik dostępu (plik z rozszerzeniem FDERTR) utworzony i wysłany przez administratora korporacyjnej sieci LAN (patrz instrukcje poniżej).

e. Pobierz plik dostępu w oknie **Pobierz klucz dostępu do urządzenia**.

9. Jeśli odszyfrowujesz urządzenie, musisz skonfigurować dodatkowe ustawienia odszyfrowywania:

- Określ deszyfrowany obszar:
 - Jeśli chcesz odszyfrować całe urządzenie, zaznacz opcję **Odszyfruj całe urządzenie**.
 - Jeśli chcesz odszyfrować część danych na urządzeniu, zaznacz opcję **Odszyfruj określone obszary urządzenia** i określ granice obszaru deszyfrowania.
- Wybierz miejsce zapisu odszyfrowanych danych:
 - Jeśli chcesz, żeby dane na oryginalnym urządzeniu były nadpisane odszyfrowanymi danymi, odznacz pole **Odszyfruj do pliku obrazu dysku**.
 - Jeśli chcesz zapisać odszyfrowane dane w innym miejscu niż oryginalne, zaszyfrowane dane, zaznacz pole **Odszyfruj do pliku obrazu dysku** i użyj przycisku **Przełóżaj**, aby określić miejsce zapisu pliku VHD.

10. Kliknij **OK**.

Proces odblokowania / deszyfrowania urządzenia zostanie uruchomiony.

[Jak utworzyć zaszyfrowany plik dostępu do danych w Konsoli administracyjnej \(MMC\)?](#) 

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W drzewie Konsoli administracyjnej wybierz kolejno **Dodatkowe** → **Ochrona i szyfrowanie danych** → **Zaszyfrowane dyski**.
3. W obszarze roboczym wybierz zaszyfrowane urządzenie, dla którego chcesz utworzyć plik klucza dostępu, a z menu kontekstowego urządzenia wybierz **Uzyskaj dostęp do urządzenia z poziomu Kaspersky Endpoint Security for Windows**.

Jeśli nie jesteś pewien, dla którego komputera został wygenerowany plik żądania dostępu, w drzewie Konsoli administracyjnej wybierz folder **Dodatkowe** → **Szyfrowanie i ochrona danych** i w obszarze roboczym kliknij **Uzyskaj klucz szyfrujący urządzenie z poziomu Kaspersky Endpoint Security for Windows**.

4. W oknie, które zostanie otwarte, wybierz algorytm szyfrowania, którego chcesz użyć: **AES256** lub **AES56**.
Algorytm szyfrowania danych zależy od biblioteki szyfrowania AES zawartej w pakiecie dystrybucyjnym: *Silne szyfrowanie (AES256)* lub *Uproszczone szyfrowanie (AES56)*. Biblioteka szyfrowania AES jest instalowana wraz z aplikacją.
5. Kliknij **Przeglądaj**, aby otworzyć okno; w tym oknie określ ścieżkę do pliku żądania z rozszerzeniem fdertc, które zostało otrzymane od użytkownika.
6. Kliknij przycisk **Otwórz**.

Zobaczysz informacje o żądaniu użytkownika. Kaspersky Security Center wygeneruje plik klucza. Wyślij do użytkownika wygenerowany plik klucza dostępu do zaszyfrowanych danych. Lub zapisz plik dostępu i użyj dowolnej dostępnej metody, aby przenieść plik.

[Jak utworzyć zaszyfrowany plik dostępu do danych w konsoli Web Console?](#) 

1. W oknie głównym konsoli Web Console wybierz **Operacje** → **Szyfrowanie i ochrona danych** → **Zaszyfrowane dyski**.

2. Zaznacz pole wyboru obok nazwy komputera, na którym chcesz odzyskać dane.

3. Kliknij przycisk **Udziel dostępu do urządzenia w trybie offline**.

Spowoduje to uruchomienie Kreatora umożliwiającego uzyskanie dostępu do urządzenia.

4. Postępuj zgodnie z instrukcjami Kreatora, aby przyznać dostęp do urządzenia:

a. Wybierz wtyczkę **Kaspersky Endpoint Security for Windows**.

b. Wybierz algorytm szyfrowania, którego chcesz użyć: **AES256** lub **AES56**.

Algorytm szyfrowania danych zależy od biblioteki szyfrowania AES zawartej w pakiecie dystrybucyjnym: *Silne szyfrowanie (AES256)* lub *Uproszczone szyfrowanie (AES56)*. Biblioteka szyfrowania AES jest instalowana wraz z aplikacją.

c. Kliknij przycisk **Wybierz plik** i wybierz plik żądania dostępu otrzymany od użytkownika (plik z rozszerzeniem FDERTC).

d. Kliknij przycisk **Zapisz klucz** i wybierz folder, aby zapisać plik klucza w celu uzyskania dostępu do zaszyfrowanych danych (plik z rozszerzeniem FDERTR).

W rezultacie będziesz mógł uzyskać klucz dostępu do zaszyfrowanych danych, który będziesz musiał przekazać użytkownikowi.

Tworzenie dysku ratunkowego systemu operacyjnego

Dysk ratunkowy systemu operacyjnego może być przydatny, gdy z jakiegoś powodu nie można uzyskać dostępu do zaszyfrowanego dysku twardego, a system operacyjny nie może zostać załadowany.

Użytkownik może załadować obraz systemu operacyjnego Windows przy użyciu dysku ratunkowego oraz przywrócić dostęp do zaszyfrowanego dysku twardego przy pomocy Narzędzia przywracania zaszyfrowanego urządzenia, załączonego do obrazu systemu operacyjnego.

W celu utworzenia dysku ratunkowego systemu operacyjnego:

1. [Utwórz plik wykonywalny Narzędzia przywracania zaszyfrowanego urządzenia](#).

2. Utwórz niestandardowy obraz środowiska pre-boot systemu Windows. Podczas tworzenia niestandardowego obrazu środowiska pre-boot systemu Windows dodaj do obrazu plik wykonywalny Narzędzia przywracania zaszyfrowanego urządzenia.

3. Zapisz niestandardowy obraz środowiska preinstalacyjnego systemu Windows na dysku rozruchowym, takim jak CD lub nośnik wymienny.

Instrukcje dotyczące tworzenia niestandardowego obrazu środowiska preinstalacyjnego systemu Windows można znaleźć w plikach pomocy Microsoft (na przykład w [zasobach Microsoft TechNet](#)).

Detection and Response

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent obsługuje interakcję między aplikacją a innymi rozwiązaniami firmy Kaspersky w celu wykrywania zaawansowanych zagrożeń (np. Kaspersky Sandbox). Rozwiązania Kaspersky są kompatybilne z określonymi wersjami Kaspersky Endpoint Agent.

W celu uzyskania kompletnych informacji o Kaspersky Endpoint Agent for Windows zawartych w używanym rozwiązaniu oprogramowania oraz w celu uzyskania kompletnych informacji o rozwiązaniu autonomicznym zapoznaj się z pomocą dla odpowiedniego produktu:

- *Pomoc dla Kaspersky Anti Targeted Attack Platform*
- *Pomoc dla Kaspersky Sandbox*
- *Pomoc dla Kaspersky Endpoint Detection and Response Optimum*
- *Pomoc dla Kaspersky Managed Detection and Response*

Kaspersky Endpoint Agent znajduje się w [pakiecie dystrybucyjnym Kaspersky Endpoint Security](#). Możesz zainstalować Kaspersky Endpoint Agent podczas instalacji Kaspersky Endpoint Security. Aby to zrobić, należy wybrać składnik Endpoint Agent podczas instalacji aplikacji (na przykład, w [pakiecie instalacyjnym](#)). Po zainstalowaniu aplikacji za pomocą Endpoint Agent, Kaspersky Endpoint Security i Kaspersky Endpoint Agent zostaną dodane do listy zainstalowanych aplikacji. Po odinstalowaniu Kaspersky Endpoint Security, Kaspersky Endpoint Agent również zostanie odinstalowany automatycznie.

Teraz Kaspersky Endpoint Security 11.7.0 zawiera kreator migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security. Możesz migrować ustawienia zasady i zadania dla następujących rozwiązań:

- Kaspersky Sandbox;
- Kaspersky Endpoint Detection and Response (EDR);
- Kaspersky Managed Detection and Response (MDR).

Zalecane jest rozpoczęcie migracji Kaspersky Endpoint Agent do Kaspersky Endpoint Security na pojedynczym komputerze, następnie zrób to na grupie komputerów, a następnie zakończ migrację na wszystkich komputerach w organizacji.

W celu migracji ustawień zasady i zadania z Kaspersky Endpoint Agent do Kaspersky Endpoint Security:

W oknie głównym Web Console wybierz **Operacje** → **Migracja z Kaspersky Endpoint Agent**.

To spowoduje uruchomienie Kreatora migracji zasady i zadania. Postępuj zgodnie z instrukcjami Kreatora.

Krok 1. Migracja zasady

Kreator migracji tworzy nową zasadę, która scala ustawienia zasad Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Na liście zasad wybierz zasady Kaspersky Endpoint Agent, których ustawienia chcesz scalić z zasadą Kaspersky Endpoint Security. Kliknij zasadę Kaspersky Endpoint Agent, aby wybrać Kaspersky Endpoint Security, z którym chcesz scalić ustawienia. Upewnij się, że wybrałeś poprawne zasady i przejdź do następnego kroku.

Krok 2. Migracja zadania

Kreator migracji tworzy nowe zadania dla Kaspersky Endpoint Security. Na liście zadań wybierz zadania Kaspersky Endpoint Agent, które chcesz utworzyć dla zasady Kaspersky Endpoint Security. Kreator obsługuje zadania dla Kaspersky Endpoint Detection and Response i dla Kaspersky Sandbox. Przejdź do następnego kroku.

Krok 3. Kończenie działania kreatora

Zakończ działanie Kreatora. W wyniku tego działania kreator:

- Utworzy nową zasadę Kaspersky Endpoint Security.

Zasada scala ustawienia z Kaspersky Endpoint Security i Kaspersky Endpoint Agent. Zasada zostaje nazwana <Nazwa zasady Kaspersky Endpoint Security> & <Nazwa zasady Kaspersky Endpoint Agent>. Nowa zasada posiada stan *Nieaktywny*. Aby kontynuować, zmień stany zasad Kaspersky Endpoint Agent i Kaspersky Endpoint Security na *Nieaktywny* i aktywuj nową scaloną zasadę.

Po migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows upewnij się, że nowa zasada posiada [funkcjonalność przesyłania danych do Serwera administracyjnego](#) (dane pliku poddanego kwarantannie oraz dane łańcucha rozwoju zagrożeń). Wartości parametrów przesyłania danych nie zostają przeniesione z zasady Kaspersky Endpoint Agent.

- Utworzy nowe zadania Kaspersky Endpoint Security.

Nowe zadania są kopiami zadań Kaspersky Endpoint Agent dla Kaspersky Endpoint Detection and Response i Kaspersky Sandbox. Jednocześnie kreator pozostawia zadania Kaspersky Endpoint Agent niezmienione.

Migrowanie konfiguracji [KES+KEA] do [KES11.7.0]

Teraz Kaspersky Endpoint Security 11.7.0 posiada wbudowane agenty dla rozwiązań Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum) oraz Kaspersky Sandbox 2.0. Nie potrzebujesz już oddzielnej aplikacji Kaspersky Endpoint Agent do pracy z tymi rozwiązaniami. Jeśli aktualizujesz Kaspersky Endpoint Security do wersji 11.7.0, rozwiązania EDR Optimum i Kaspersky Sandbox działają z Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent jest usuwany z komputera.

Migrowanie konfiguracji [KES+KEA] do [KES11.7.0] obejmuje następujące etapy:

1 Aktualizowanie Kaspersky Security Center

Zaktualizuj wszystkie komponenty Kaspersky Security Center do wersji 13.2, w tym Agenta administracyjnego na komputerach użytkowników i Web Console.

2 Aktualizowanie wtyczki webowej Kaspersky Endpoint Security

W Kaspersky Security Center Web Console zaktualizuj wtyczkę webową Kaspersky Endpoint Security do wersji 11.7.0. Aby zarządzać komponentami EDR Optimum i Kaspersky Sandbox, musisz korzystać z Web Console.

3 Migrowanie zasady i zadań

Użyj [Kreatora migracji zadań i zasad Kaspersky Endpoint Agent](#), aby przenieść ustawienia Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows.

To spowoduje utworzenie nowej zasady Kaspersky Endpoint Security. Nowa zasada posiada stan *Nieaktywny*. Aby zastosować zasadę, otwórz właściwości zasady, zaakceptuj Oświadczenie Kaspersky Security Network i ustaw stan na *Aktywny*.

4 Funkcjonalność licencjonowania

Jeśli do aktywowania Kaspersky Endpoint Security for Windows i Kaspersky Endpoint Agent używasz wspólnej licencji dla Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security, funkcjonalność EDR Optimum zostanie aktywowana automatycznie po zaktualizowaniu aplikacji do wersji 11.7.0. Nie musisz robić nic innego.

Jeśli do aktywowania funkcjonalności EDR Optimum używasz autonomicznej licencji Kaspersky Endpoint Detection and Response Optimum Add-on, musisz upewnić się, że klucz EDR Optimum zostanie dodany do repozytorium Kaspersky Security Center, a [funkcjonalność automatycznej dystrybucji klucza licencyjnego zostanie włączona](#). Po zaktualizowaniu aplikacji do wersji 11.7.0, funkcjonalność EDR Optimum zostanie aktywowana automatycznie.

Jeśli do aktywowania Kaspersky Endpoint Agent użyjesz licencji dla Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security, a do aktywowania Kaspersky Endpoint Security for Windows użyjesz innej licencji, musisz zastąpić klucz Kaspersky Endpoint Security for Windows standardowym kluczem Kaspersky Endpoint Detection and Response Optimum lub Kaspersky Optimum Security. Możesz zastąpić klucz przy użyciu zadania [Dodaj klucz](#).

Nie musisz aktywować funkcjonalności Kaspersky Sandbox. Funkcjonalność Kaspersky Sandbox będzie dostępna natychmiast po zaktualizowaniu i aktywowaniu Kaspersky Endpoint Security for Windows.

5 Aktualizowanie aplikacji Kaspersky Endpoint Security

Aby zaktualizować aplikację i migrować funkcję EDR Optimum i Kaspersky Sandbox, zalecane jest wykonanie [zadania zdalnej instalacji](#).

W celu zaktualizowania aplikacji przy użyciu zadania zdalnej instalacji, musisz edytować następujące ustawienia:

- W ustawieniach pakietu instalacyjnego wybierz komponenty Endpoint Detection and Response Optimum lub Kaspersky Sandbox.
- Wyklucz komponent Kaspersky Endpoint Agent w ustawieniach pakietu instalacyjnego.

Możesz także zaktualizować aplikację za pomocą następujących metod:

- Przy użyciu usługi aktualizacji Kaspersky (Seamless Update – SMU).
- Lokalnie, za pomocą Kreatora instalacji.

W tym przypadku musisz sprawdzić konfigurację programu Kaspersky Endpoint Agent, który jest zainstalowany na komputerze. Jeśli zainstalowany agent Kaspersky Endpoint Agent zawiera komponent Endpoint Detection and Response Expert (KATA EDR), usuń komponent przed aktualizacją aplikacji. Jeśli nie możesz usunąć komponentu Endpoint Detection and Response Expert (KATA EDR), podczas aktualizacji aplikacji Kaspersky Endpoint Security pominie komponenty EDR Optimum i Kaspersky Sandbox. Po zaktualizowaniu aplikacji możesz zainstalować komponenty, korzystając z zadania [Zmiana składników aplikacji](#).

6 Ponowne uruchomienie komputera

Uruchom ponownie komputer, aby zakończyć aktualizowanie aplikacji za pomocą wbudowanego agenta. Podczas aktualizowania aplikacji instalator usuwa Kaspersky Endpoint Agent przed ponownym uruchomieniem komputera. Po ponownym uruchomieniu komputera instalator dodaje wbudowanego agenta. Oznacza to, że Kaspersky Endpoint Security nie będzie pełnił funkcji EDR i Kaspersky Sandbox do momentu ponownego uruchomienia komputera.

7 Sprawdzanie zdrowia Kaspersky Endpoint Detection and Response Optimum i Kaspersky Sandbox

Jeśli po aktualizacji, komputer posiada stan *Krytyczny* w konsoli Kaspersky Security Center:

- Upewnij się, że na komputerze jest zainstalowany Agent administracyjny 13.2.
- Sprawdź stan działania komponentów EDR Optimum i Kaspersky Sandbox, przeglądając *Raport dotyczący stanu komponentów aplikacji*. Jeśli komponent posiada stan *Nie zainstalowano*, zainstaluj komponenty przy użyciu zadania [Zmiana składników aplikacji](#).
- Upewnij się, że akceptujesz Oświadczenie Kaspersky Security Network w nowej zasadzie Kaspersky Endpoint Security for Windows.

Upewnij się, że funkcjonalność EDR Optimum została aktywowana przy użyciu *Raportu dotyczącego stanu komponentów aplikacji*. Jeśli komponent posiada stan *Nie objęty licencją*, upewnij się, że [funkcjonalność automatycznej dystrybucji klucza licencyjnego EDR Optimum jest włączona](#).

Aktualizowanie aplikacji jako części KATA EDR

Jeśli posiadasz zainstalowany program Kaspersky Endpoint Agent do integracji z Kaspersky Anti Targeted Attack Platform (komponent Endpoint Detection and Response Expert (KATA EDR)), możesz zaktualizować Kaspersky Endpoint Security for Windows w jeden z następujących sposobów:

- Przy użyciu zadania zdalnej instalacji.

W tym celu należy edytować następujące ustawienia:

- W ustawieniach pakietu instalacyjnego wyklucz komponenty Endpoint Detection and Response Optimum i Kaspersky Sandbox.
- W ustawieniach pakietu instalacyjnego wybierz komponent Kaspersky Endpoint Agent. Jeśli komputer posiada już zainstalowany program Kaspersky Endpoint Agent, aplikacja zostanie zaktualizowana do wersji 3.11.

- Przy użyciu usługi aktualizacji Kaspersky (SMU).

Aby to zrobić, należy potwierdzić aktualizację aplikacji. Kaspersky Endpoint Security wykluczy Endpoint Detection and Response Optimum i Kaspersky Sandbox z instalacji. Aktualizowanie Kaspersky Endpoint Agent nie jest obsługiwane. Możesz ręcznie zaktualizować Kaspersky Endpoint Agent.

- Lokalnie, za pomocą Kreatora instalacji.

Kaspersky Endpoint Security wykluczy Endpoint Detection and Response Optimum i Kaspersky Sandbox z instalacji. Jeśli komputer posiada już zainstalowany program Kaspersky Endpoint Agent, aplikacja zostanie zaktualizowana do wersji 3.11.

Managed Detection and Response



W Kaspersky Endpoint Security 11.6.0 wprowadzono wbudowanego agenta dla rozwiązania Managed Detection and Response. Rozwiązanie *Kaspersky Managed Detection and Response (MDR)*

automatycznie wykrywa i analizuje incydenty naruszenia bezpieczeństwa w Twojej infrastrukturze. W tym celu MDR używa danych telemetrycznych, otrzymanych z punktów końcowych i uczenia maszynowego. MDR wysyła dane incydentu do ekspertów z Kaspersky. Ekspersi mogą następnie przetworzyć incydent i, na przykład, dodać nowy wpis do antywirusowych baz danych. Zamiast tego eksperci mogą opublikować zalecenia odnośnie przetwarzania incydentu i, na przykład, zasugerować odizolowanie komputera od sieci. Szczegółowe informacje dotyczące sposobu działania rozwiązania można znaleźć w [pomocy do Kaspersky Managed Detection and Response](#).

Podczas interakcji z Kaspersky Managed Detection and Response aplikacja umożliwi wykonanie następujących czynności:

- Aktywuj Managed Detection and Response przy użyciu pliku konfiguracyjnego BLOB.
- Wykonaj polecenia z Kaspersky Managed Detection and Response.
- Wyślij dane telemetryczne do Kaspersky Managed Detection and Response w celu wykrycia zagrożeń.

Integracja z Kaspersky Managed Detection and Response

Integracja z Kaspersky Managed Detection and Response obejmuje następujące kroki:

1 Konfigurowanie prywatnej sieci Kaspersky Security Network

Pomiń ten krok, jeśli używasz Kaspersky Security Center Cloud Console. Kaspersky Security Center Cloud Console automatycznie konfiguruje lokalną sieć Kaspersky Security Network podczas instalowania wtyczki MDR.

Prywatna sieć KSN obsługuje wymianę danych między komputerami a dedykowanymi serwerami Kaspersky Security Network, ale nie globalną siecią KSN.

Wczytaj plik konfiguracyjny Kaspersky Security Network we właściwościach Serwera administracyjnego. Plik konfiguracyjny Kaspersky Security Network znajduje się w archiwum ZIP pliku konfiguracyjnego MDR. Archiwum ZIP możesz uzyskać w Kaspersky Managed Detection and Response Console. Więcej informacji na temat konfiguracji prywatnej sieci Kaspersky Security Network można znaleźć w [pomocy do Kaspersky Security Center](#). Plik konfiguracyjny Kaspersky Security Network możesz wczytać także z poziomu wiersza polecenia (zapoznaj się z poniższymi instrukcjami).

[Jak skonfigurować prywatną sieć Kaspersky Security Network z poziomu wiersza polecenia?](#)

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się pakiet dystrybucyjny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:

```
avp.com KSN /private <nazwa pliku>
```

gdzie <nazwa pliku> to nazwa pliku konfiguracyjnego zawierającego ustawienia prywatnej sieci KSN (format pliku PKCS7 lub PEM).

Na przykład:

```
avp.com KSN /private C:\kpsn_config.pkcs7
```

W wyniku tego działania Kaspersky Endpoint Security będzie używał Prywatnej sieci KSN do określenia reputacji plików, aplikacji i stron internetowych. Ustawienia zasady w sekcji **Kaspersky Security Network** wyświetlą następujący stan działania: *Sieć KSN: Prywatna sieć KSN*.

Musisz [włączyć rozszerzony tryb KSN](#) dla Managed Detection and Response, aby działało.

2 Aktywuj Managed Detection and Response

Załaduj plik konfiguracyjny BLOB w zasadzie Kaspersky Endpoint Security (zapoznaj się z poniższymi instrukcjami). Plik BLOB zawiera ID klienta oraz informacje o licencji dla Kaspersky Managed Detection and Response. Plik BLOB znajduje się w archiwum ZIP pliku konfiguracyjnego MDR. Archiwum ZIP możesz uzyskać w Kaspersky Managed Detection and Response Console. Więcej informacji o pliku BLOB *można znaleźć w [pomocy dla Kaspersky Managed Detection and Response](#)*.

[Jak aktywować Managed Detection and Response w Konsoli administracyjnej.\(MMC\)?](#)

1. Otwórz Konsolę administracyjną Kaspersky Security Center.
2. W folderze **Zarządzane urządzenia** z drzewa Konsoli administracyjnej otwórz folder grupy administracyjnej, do której należą wybrane komputery klienckie.
3. W obszarze roboczym wybierz zakładkę **Profile**.
4. Wybierz żądany profil i kliknij go dwukrotnie, aby otworzyć właściwości profilu.
5. W oknie zasady wybierz **Detection and Response** → **Managed Detection and Response**.
6. Zaznacz pole **Managed Detection and Response**.
7. W sekcji **Ustawienia** kliknij **Importuj** i wybierz plik BLOB pobrany w Kaspersky Managed Detection and Response Console. Plik posiada rozszerzenie P7.
8. Zapisz swoje zmiany.

[Jak aktywować Managed Detection and Response w Web Console i Cloud Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Detection and Response** → **Managed Detection and Response**.
5. Włącz przełącznik **Managed Detection and Response**.
6. Kliknij **Importuj** i wybierz plik BLOB, który został uzyskany w Kaspersky Managed Detection and Response Console. Plik posiada rozszerzenie P7.
7. Zapisz swoje zmiany.

[Jak aktywować Managed Detection and Response z poziomu wiersza polecenia?](#)

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się pakiet dystrybucyjny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:
 - Jeśli ustawienia aplikacji nie są [chronione hasłem](#):
avp.com MDRLICENSE /ADD <nazwa pliku>
<Nazwa pliku> to nazwa pliku konfiguracyjnego BLOB do aktywacji Managed Detection and Response (format pliku P7).
 - Jeśli ustawienia aplikacji są [chronione hasłem](#):
avp.com MDRLICENSE /ADD <nazwa pliku> /login=<nazwa użytkownika> /password=<hasło>

W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał plik BLOB. Weryfikacja pliku BLOB obejmuje sprawdzanie podpisu cyfrowego i okresu licencjonowania. Jeśli plik BLOB został pomyślnie zweryfikowany, Kaspersky Endpoint Security wczyta plik i wyśle go do komputera podczas kolejnej synchronizacji z Kaspersky Security Center. Sprawdź stan działania komponentu, przeglądając *Raport dotyczący stanu komponentów aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Managed Detection and Response** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

3 Obsługiwanie Managed Detection and Response

Musisz włączyć następujące komponenty dla Managed Detection and Response w celu zapewnienia działania:

- [Kaspersky Security Network \(tryb rozszerzony\)](#).
- [Wykrywanie zachowań](#).

Włączenie tych komponentów jest nieopcjonalne. W innym przypadku Kaspersky Managed Detection and Response nie może działać, ponieważ nie pobiera wymaganych danych telemetrycznych.

Dodatkowo, Kaspersky Managed Detection and Response wykorzystuje dane otrzymane od innych komponentów aplikacji. Włączenie tych komponentów jest opcjonalne. Komponenty, które udostępniają dodatkowe dane, zawierają:

- [Ochrona WWW](#).
- [Ochrona poczty](#).
- [Zapora sieciowa](#).

Aby rozwiązanie Kaspersky Managed Detection and Response działało z Serwerem administracyjnym poprzez Kaspersky Security Center Web Console, należy także nawiązać nowe bezpieczne połączenie - *połączenie w tle*. Kaspersky Managed Detection and Response wyświetla pytanie o nawiązanie połączenia w tle po wdrożeniu rozwiązania. Upewnij się, że połączenie w tle zostało nawiązane. Więcej informacji o integracji Kaspersky Security Center z innymi rozwiązaniami Kaspersky można znaleźć w [pomocy dla Kaspersky Security Center](#).

Migracja z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security w wersji 11 i nowszej obsługuje rozwiązanie MDR. Kaspersky Endpoint Security w wersjach 11 – 11.5.0 tylko wysyła dane telemetryczne Kaspersky Managed Detection and Response, aby włączyć wykrywanie zagrożeń. Kaspersky Endpoint Security w wersji 11.6.0 posiada pełną funkcjonalność agenta wbudowanego (Kaspersky Endpoint Agent).

Jeśli korzystasz z Kaspersky Endpoint Security 11 – 11.5.0, musisz zaktualizować bazy danych do najnowszej wersji w celu pracy z rozwiązaniem MDR. Musisz także zainstalować Kaspersky Endpoint Agent.

Jeśli korzystasz z Kaspersky Endpoint Security 11.6.0 lub nowszej wersji, do pracy z rozwiązaniem MDR, podczas instalowania aplikacji musisz wybrać komponent Managed Detection and Response. W tym przypadku nie musisz instalować Kaspersky Endpoint Agent.

W celu migracji z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows:

1. Konfiguruj integrację z Kaspersky Managed Detection and Response w zasadzie Kaspersky Endpoint Security.
2. Wyłącz komponent Managed Detection and Response w zasadzie Kaspersky Endpoint Agent.

Jeśli zasada Kaspersky Endpoint Security także jest stosowana także do komputerów, na których nie jest zainstalowany program Kaspersky Endpoint Security 11 – 11.5.0, w pierwszej kolejności musisz utworzyć oddzielną zasadę Kaspersky Endpoint Agent dla tych komputerów. W nowej zasadzie skonfiguruj integrację z Kaspersky Managed Detection and Response.

Endpoint Detection and Response



Kaspersky Endpoint Security 11.7.0 posiada teraz wbudowanego agenta dla rozwiązania Kaspersky Endpoint Detection and Response Optimum (zwane dalej „EDR Optimum”). *Kaspersky Endpoint Detection and Response Optimum* to rozwiązanie do ochrony infrastruktury IT organizacji przed zaawansowanymi cyberzagrożeniami. Funkcjonalność rozwiązania łączy automatyczne wykrywanie zagrożeń z możliwością reagowania na te zagrożenia w celu przeciwdziałania zaawansowanym atakom, w tym nowym exploitom, oprogramowaniu ransomware, atakom bezplikowym, a także metodom z użyciem legalnych narzędzi systemowych. Więcej informacji o rozwiązaniu znajdziesz w [pomocy dla Kaspersky Endpoint Detection and Response Optimum](#).

Kaspersky Endpoint Detection and Response Optimum przegląda i analizuje rozwój zagrożeń i zapewnia *personel ds. bezpieczeństwa* lub *Administratora* z informacjami o potencjalnym ataku, które są niezbędne do reagowania w odpowiednim momencie. Kaspersky Endpoint Detection and Response wyświetla szczegóły wykrycia w oddzielnym oknie. *Szczegóły wykrycia* to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu i zarządzaniu działaniami odpowiedzi. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do [Kaspersky Endpoint Detection and Response Optimum](#).

Rozwiązanie używa następujących narzędzi analizy zagrożeń:

- Infrastruktura usługi chmury Kaspersky Security Network (zwana dalej również „KSN”), która zapewnia dostęp do informacji o reputacji pliku, strony internetowej i oprogramowania w czasie rzeczywistym z bazy wiedzy Kaspersky. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi aplikacji firmy Kaspersky na zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie prawdopodobieństwa wystąpienia fałszywych alarmów.
- Integracja z Kaspersky Private Security Network (zwane dalej także „KPSN”), co umożliwia użytkownikowi uzyskanie dostępu do bazy danych reputacji KSN, a także innych danych statystycznych bez wysyłania danych z ich komputerów do KSN.

- Integracja z systemem informacji Kaspersky Threat Intelligence Portal, który zawiera i wyświetla informacje o reputacji plików i adresów internetowych.
- Baza danych Kaspersky Threats.

Kaspersky Endpoint Detection and Response Optimum wymaga Kaspersky Security Center w wersji 13.2. We wcześniejszych wersjach Kaspersky Security Center nie ma możliwości aktywowania funkcji EDR Optimum.

Komponent może być zarządzany tylko przy użyciu konsoli Web Console. Nie możesz zarządzać tym komponentem przy użyciu Konsoli administracyjnej (MMC).

Integracja z Kaspersky Endpoint Detection and Response Optimum

Integracja z Kaspersky Endpoint Detection and Response Optimum obejmuje następujące etapy:

1 Zainstalowanie komponentu Kaspersky Endpoint Detection and Response Optimum

Możesz wybrać komponent Endpoint Detection and Response Optimum podczas [instalacji](#) lub [aktualizacji](#), a także przy użyciu zadania [Zmiana składników aplikacji](#).

Po wykonaniu zadania *Zmiana składników aplikacji* stan zadania zostanie wyświetlony niepoprawnie. Zamiast *Zakończono pomyślnie* zadanie posiada stan *Zaplanowane*. Jednakże zadanie może nadal zostać zakończone pomyślnie. Upewnij się, że nowy składnik został zainstalowany we właściwościach komputera konsoli Kaspersky Security Center (**Aplikacje** → **Kaspersky Endpoint Security for Windows** → **Components**) lub w lokalnym interfejsie aplikacji.

2 Aktywowanie Kaspersky Endpoint Detection and Response Optimum

Możesz uzyskać licencję do korzystania z Kaspersky Endpoint Detection and Response Optimum na następujące sposoby:

- Funkcja EDR Optimum znajduje się w licencji dla korzystania z Kaspersky Endpoint Security for Windows.

Funkcja będzie dostępna natychmiast po [aktywacji Kaspersky Endpoint Security for Windows](#).

- Rozszerzenie licencji dla korzystania z EDR Optimum.

Funkcja będzie dostępna po dodaniu oddzielnego klucza dla Kaspersky Endpoint Detection and Response. W rezultacie na komputerze zostaną zainstalowane dwa klucze: klucz dla Kaspersky Endpoint Security i klucz dla Kaspersky Endpoint Detection and Response Optimum.

Licencjonowanie dla indywidualnej funkcji EDR Optimum nie różni się od licencjonowania dla Kaspersky Endpoint Security.

Upewnij się, że funkcja EDR Optimum znajduje się w licencji i jest uruchomiona w [lokalnym interfejsie aplikacji](#).

3 Włączenie komponentu Endpoint Detection and Response Optimum

Możesz włączyć lub wyłączyć komponent w ustawieniach zasady Kaspersky Endpoint Security for Windows.

W celu użycia komponentu spełnione muszą być następujące warunki:

- Aplikacja jest aktywowana, a funkcja Kaspersky Endpoint Detection and Response Optimum jest objęta licencją.
- Komponent Endpoint Detection and Response Optimum jest włączony.

- Składniki aplikacji, od których zależy Endpoint Detection and Response Optimum, są włączone i działają. Komponent zależy od następujących komponentów:
 - [Ochrona plików.](#)
 - [Ochrona WWW.](#)
 - [Ochrona poczty.](#)
 - [Ochrona przed exploitami.](#)
 - [Wykrywanie zachowań.](#)
 - [Ochrona przed włamaniami.](#)
 - [Silnik korygujący.](#)
 - [Adaptacyjna kontrola anomalii.](#)

[Jak w konsoli Web Console włączyć lub wyłączyć komponent Endpoint Detection and Response Optimum?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Detection and Response** → **Endpoint Detection and Response Optimum**.
5. Włącz przełącznik **Endpoint Detection and Response Optimum**.
6. Zapisz swoje zmiany.

Komponent Kaspersky Endpoint Detection and Response Optimum jest włączony. Sprawdź stan działania komponentu, przeglądając *Raport dotyczący stanu komponentów aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Endpoint Detection and Response Optimum** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

4 Włączanie przesyłania danych do Serwera administracyjnego

W celu włączenia wszystkich funkcji EDR Optimum, przesyłanie powinno być włączone dla następujących typów danych:

- Dane pliku poddanego kwarantannie.
Dane są wymagane do uzyskania informacji o plikach poddanych kwarantannie na komputerze za pośrednictwem Web Console. Na przykład, możesz pobrać plik z kwarantanny do analizy w Web Console.
- Dane łańcucha rozwoju zagrożeń.
Dane są wymagane do uzyskania informacji o zagrożeniach wykrytych na komputerze w Web Console. Możesz przejrzeć szczegóły powiadomień i podjąć działanie w Web Console.

[Jak włączyć przesyłanie danych do Serwera administracyjnego w Web Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia główne** → **Raporty i pliki danych**.
5. W sekcji **Przesyłanie danych do Serwera administracyjnego** zaznacz następujące pola:
 - **Informacje o plikach poddanych kwarantannie**.
 - **Informacje o łańcuchu rozwoju zagrożeń**.
6. Zapisz swoje zmiany.

Migracja z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows

Jeśli używasz Kaspersky Endpoint Security 11.7.0 lub nowszej wersji z zainstalowanym komponentem EDR Optimum (wbudowany agent), nie musisz nic robić, aby rozwiązanie Kaspersky Endpoint Detection and Response Optimum działało. Komponent EDR Optimum nie jest kompatybilny z Kaspersky Endpoint Agent. Jeśli Kaspersky Endpoint Agent jest zainstalowany na komputerze, po zaktualizowaniu Kaspersky Endpoint Security do wersji 11.7.0, Kaspersky Endpoint Detection and Response Optimum dalej działa z Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent zostanie usunięty z komputera. Aby zakończyć migrację z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows, musisz przenieść ustawienia zasady i zadania przy pomocy [Kreatora migracji](#).

Jeśli używasz Kaspersky Endpoint Security 11.4.0–11.6.0 do współdziałania z Kaspersky Endpoint Detection and Response Optimum, aplikacja zawiera Kaspersky Endpoint Agent. Możesz zainstalować Kaspersky Endpoint Agent wraz z Kaspersky Endpoint Security.

Komponent EDR Optimum jako część Kaspersky Endpoint Security obsługuje interakcję z rozwiązaniem Kaspersky Endpoint Detection and Response Optimum 2.0. Interakcja z Kaspersky Endpoint Detection and Response Optimum w wersji 1.0 nie jest obsługiwana.

Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (IOC)

Wskaźnik naruszeń bezpieczeństwa (IOC) to zestaw danych dotyczących obiektu lub aktywności, która wskazuje nieautoryzowany dostęp do komputera (naruszenie bezpieczeństwa danych). Na przykład, wiele niepomyślnych prób zalogowania do systemu może stanowić wskaźnik naruszeń bezpieczeństwa. Zadania *Skanowanie IOC* umożliwiają odszukanie wskaźników naruszeń bezpieczeństwa na komputerze i podejmują środki reakcji na zagrożenia.

Kaspersky Endpoint Security wyszukuje wskaźniki naruszeń bezpieczeństwa przy użyciu plików IOC *Pliki IOC* to pliki zawierające zestawy wskaźników, które aplikacja próbuje dopasować w celu policzenia wykryć. Pliki IOC muszą pasować do [standardu OpenIOC](#). Kaspersky Endpoint Security automatycznie tworzy pliki IOC i zezwala na załadowanie plików IOC przygotowanych przez użytkownika. Jeśli chcesz ręcznie dodać wskaźnik naruszenia bezpieczeństwa, zapoznaj się z [wymaganiami plików IOC](#).

Plik, który możesz pobrać, klikając poniższy odnośnik, zawiera tabelę z pełną listą warunków IOC standardu OpenIOC, który jest obsługiwany przez rozwiązanie Kaspersky Endpoint Detection and Response.

 [POBIERZ PLIK IOC TERMS.XLSX](#)

Tryby uruchamiania zadania Skanowanie IOC

Kaspersky Endpoint Security umożliwia uruchomienie *Skanowania IOC* w następujących trybach:

- *Standardowe zadanie skanowania IOC* to zadanie grupowe lub lokalne, które jest tworzone i skonfigurowane ręcznie w konsoli Web Console. Zadania są uruchamiane przy użyciu plików IOC przygotowanych przez użytkownika.
- *Autonomiczne zadanie skanowania IOC* to zadanie grupowe, które jest tworzone automatycznie podczas reagowania na zagrożenie wykryte przez [Kaspersky Sandbox](#). Kaspersky Endpoint Security automatycznie generuje plik IOC. Niestandardowe pliki IOC nie są obsługiwane. Zadania są automatycznie usuwane w ciągu siedmiu dni od ostatniego uruchomienia lub utworzenia, jeśli zadanie nie zostało nigdy uruchomione. Więcej informacji o autonomicznych zadaniach skanowania IOC możesz znaleźć w *pomocy dla* [Kaspersky Sandbox](#).

Uruchamia zadanie skanowania IOC

Kaspersky Sandbox może tworzyć zadania *Skanowanie IOC* automatycznie po reakcji na zagrożenia. W Kaspersky Endpoint Detection and Response Optimum możesz tylko ręcznie tworzyć zadania *Skanowanie IOC*.

Możesz ręcznie utworzyć zadania *Skanowanie IOC*:

- W szczegółach wykrycia.

Szczegóły wykrycia to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu i zarządzaniu działaniami odpowiedzi. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do [Kaspersky Endpoint Detection and Response Optimum](#).
- Korzystanie z Kreatora tworzenia zadania.

Możesz skonfigurować ustawienia tylko w Web Console.

Aby utworzyć autonomiczne zadania Skanowanie IOC w celu reakcji na zagrożenia, wymagany jest program Kaspersky Security Center w wersji 13.2.

W celu utworzenia zadania Skanowanie IOC:

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Kliknij przycisk **Dodaj**.
Zostanie uruchomiony Kreator tworzenia zadania.
3. Skonfiguruj ustawienia zadania:

- a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.
 - b. Na liście rozwijalnej **Typ zadania** wybierz **Skanowanie IOC**.
 - c. W polu **Nazwa zadania** wpisz krótki opis.
 - d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.
4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.
 5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij przycisk **Dalej**.

Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

Konto systemowe (SYSTEM) nie posiada uprawnień do wykonywania zadania *Skanowanie IOC* na dyskach sieciowych. Jeśli chcesz uruchomić zadanie dla dysku sieciowego, wybierz konto użytkownika, który posiada dostęp do tego dysku.

W przypadku autonomicznych zadań Skanowanie IOC na dyskach sieciowych, we właściwościach zadania należy ręcznie wybrać konto użytkownika, które ma dostęp do tego dysku.

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.
Nowe zadanie zostanie wyświetlone na liście zadań.
 7. Kliknij nowe zadanie.
Zostanie otwarte okno właściwości zadania.
 8. Wybierz zakładkę **Ustawienia aplikacji**.
 9. Przejdź do sekcji **Ustawienia skanowania IOC**.
 10. Wczytaj pliki IOC, aby wyszukać wskaźniki naruszeń bezpieczeństwa.
Po załadowaniu plików IOC, możesz przejrzeć listę wskaźników z plików IOC. Jeśli to konieczne, możesz tymczasowo wykluczyć pliki IOC z obszaru zadania.
- Dodanie lub usunięcie plików IOC po uruchomieniu zadania nie jest zalecane. To może spowodować niepoprawne wyświetlenie wyników skanowania IOC przed wcześniejszymi uruchomieniami zadania. Aby wyszukać wskaźniki naruszeń bezpieczeństwa przez nowe pliki IOC, zalecane jest dodanie nowych zadań.
11. Skonfiguruj akcje po wykryciu IOC:
 - **Odizoluj komputer od sieci**. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security odizoluje komputer od sieci, aby zapobiec rozprzestrzenianiu się zagrożenia. Możesz skonfigurować czas trwania izolacji w [ustawieniach komponentu Endpoint Detection and Response](#).
 - **Przenieś kopię do Kwarantanny, usuń obiekt**. Jeśli ta opcja została zaznaczona, Kaspersky Endpoint Security usunie szkodliwy obiekt wykryty na komputerze. Przed usunięciem obiektu Kaspersky Endpoint Security utworzy kopię zapasową w przypadku, gdy obiekt musi zostać przywrócony w późniejszym czasie. Kaspersky Endpoint Security przeniesie kopię zapasową do Kwarantanny.

- **Uruchom skanowanie obszarów krytycznych.** Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security uruchamia zadanie [Skanowanie obszarów krytycznych](#). Domyślnie, Kaspersky Endpoint Security skanuje pamięć jądra, uruchomione procesy i sektory startowe dysku.

12. Przejdź do sekcji **Zaawansowane**.

13. Wybierz typy danych (dokumenty IOC), które muszą zostać przeanalizowane jako część zadania.

Kaspersky Endpoint Security automatycznie wybiera typy danych (dokumenty IOC) dla zadania *Skanowanie IOC* zgodnie z zawartością załadowanych plików IOC. Nie jest zalecane odznaczenie typów danych.

Dodatkowo możesz skonfigurować obszary skanowania dla następujących typów danych:

- **Pliki - FileItem.** Ustaw obszar skanowania IOC na komputerze przy użyciu predefiniowanych obszarów. Domyślnie, Kaspersky Endpoint Security skanuje pod kątem wskaźników naruszeń bezpieczeństwa tylko ważne obszary komputera, takie jak folder Pobrane, pulpit, folder z tymczasowymi plikami systemu operacyjnego itd. Możesz także ręcznie dodać obszar skanowania.
- **Dziennik zdarzeń Windows - EventLogItem.** Wprowadź czas zarejestrowania zdarzeń. Możesz także wybrać dzienniki zdarzeń Windows dla skanowania IOC: dziennik zdarzeń aplikacji, dziennik zdarzeń systemu i dziennik zdarzeń ochrony.

Dla typów danych **Rejestr Windowsa - RegistryItem** Kaspersky Endpoint Security skanuje [zestaw kluczy rejestru](#).

14. Kliknij przycisk **Zapisz**.

15. Zaznacz pole obok zadania.

16. Kliknij przycisk **Uruchom**.

W rezultacie Kaspersky Endpoint Security uruchamia wyszukiwanie wskaźników naruszeń bezpieczeństwa na komputerze. Możesz przejrzeć wyniki zadania we właściwościach zadania, w sekcji **Wyniki**. Informacje o wykrytych wskaźnikach naruszeń bezpieczeństwa możesz przejrzeć we właściwościach zadania: **Ustawienia aplikacji** → **Wyniki skanowania IOC**.

Wyniki skanowania IOC są przechowywane 30 dni. Po tym czasie Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy.

Przeniesienie pliku do Kwarantanny

Podczas reagowania na zagrożenia Kaspersky Endpoint Detection and Response Optimum może utworzyć zadanie *Przeniesienie pliku do Kwarantanny*. *Kwarantanna* to specjalny lokalny magazyn na komputerze, na którym zainfekowane pliki lub pliki nie dające się wyleczyć zostają przeniesione do tego właśnie katalogu. Pliki poddane kwarantannie są przechowywane w postaci zaszyfrowanej i nie zagrażają bezpieczeństwu urządzenia. Kaspersky Endpoint Security używa Kwarantanny tylko podczas pracy z rozwiązaniami Kaspersky Sandbox i Kaspersky Endpoint Detection and Response Optimum. W innych przypadkach Kaspersky Endpoint Security umieszcza odpowiedni plik w Kopii zapasowej. Więcej informacji na temat zarządzania Kwarantanną jako częścią rozwiązań można znaleźć w [podręcznikach dotyczących Kaspersky Sandbox](#) i [Kaspersky Endpoint Detection and Response Optimum](#).

Możesz utworzyć zadania *Przenieś plik do Kwarantanny* na następujące sposoby:

- W szczegółach alertów.

Szczegóły wykrycia to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu i zarządzaniu działaniami odpowiedzi. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do [Kaspersky Endpoint Detection and Response Optimum](#) ².

- Korzystanie z Kreatora tworzenia zadania.

Musisz wprowadzić ścieżkę do pliku lub sumę kontrolną pliku (SHA256 lub MD5), albo obie te wartości.

Rozmiar pliku nie może przekraczać 100 MB.

Możesz skonfigurować ustawienia tylko w Web Console.

W celu utworzenia zadania Przenieś plik do Kwarantanny:

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

b. Na liście rozwijalnej **Typ zadania** wybierz **Przenieś plik do Kwarantanny**.

c. W polu **Nazwa zadania** wpisz krótki opis.

d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij przycisk **Dalej**.

Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. Na liście plików kliknij **Dodaj**.

Zostanie uruchomiony kreator dodawania plików.

10. Aby dodać plik, należy wprowadzić pełną ścieżkę do pliku lub zarówno sumę kontrolną, jak i ścieżkę.

Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, poczynawszy od `\\`, a nie od litery dysku. Na przykład: `\\server\shared_folder\file.exe`. Jeśli ścieżka do pliku zawiera literę dysku sieciowego, możesz uzyskać błąd *Nie odnaleziono pliku*.

11. Kliknij przycisk **Zapisz**.

12. Zaznacz pole obok zadania.

13. Kliknij przycisk **Uruchom**.

W rezultacie, Kaspersky Endpoint Security przeniesie plik do Kwarantanny. Jeśli plik jest zablokowany przez inny proces, zadanie jest wyświetlany jako *Zakończony*, ale sam plik jest poddawany kwarantannie tylko po ponownym uruchomieniu komputera. Po ponownym uruchomieniu komputera potwierdź usunięcie pliku.

Zadanie *Przenieś plik do Kwarantanny* może zostać zakończone błędem *Dostęp zabroniony*, jeśli próbujesz podać kwarantannie plik wykonywalny, który jest aktualnie uruchomiony. [Utwórz zadanie kończenia procesu](#) dla pliku i spróbuj ponownie.

Zadanie *Przenieś plik do Kwarantanny* może zakończyć się błędem *Brak wystarczającej ilości miejsca w magazynie Kwarantanny*, jeśli próbujesz podać kwarantannie plik, który jest za duży. Opróżnij Kwarantannę lub [zwiększ rozmiar Kwarantanny](#). Następnie spróbuj ponownie.

Możesz przywrócić plik z Kwarantanny lub opróżnić Kwarantannę przy użyciu konsoli Web Console. Możesz przywrócić obiekty lokalnie na komputerze przy użyciu [wiersza polecenia](#).

Uzyskaj plik

Możesz uzyskać pliki z komputerów użytkowników. Na przykład, możesz skonfigurować uzyskiwanie pliku dziennika zdarzeń, utworzonego przez aplikację innej firmy. Aby uzyskać plik, musisz utworzyć dedykowane zadanie. W wyniku wykonywania zadania plik zostanie zapisany w Kwarantannie. Możesz pobrać plik z Kwarantanny na swój komputer przy użyciu Web Console. Na komputerze użytkownika plik pozostanie w oryginalnym folderze.

Rozmiar pliku nie może przekraczać 100 MB.

Możesz skonfigurować ustawienia tylko w Web Console.

W celu utworzenia zadania Uzyskaj plik:

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

- a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.
 - b. Na liście rozwijalnej **Typ zadania** wybierz **Uzyskaj plik**.
 - c. W polu **Nazwa zadania** wpisz krótki opis.
 - d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.
4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.
 5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij przycisk **Dalej**.

Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.
Nowe zadanie zostanie wyświetlone na liście zadań.
7. Kliknij nowe zadanie.
Zostanie otwarte okno właściwości zadania.
8. Wybierz zakładkę **Ustawienia aplikacji**.
9. Na liście plików kliknij **Dodaj**.
Zostanie uruchomiony kreator dodawania plików.
10. Aby dodać plik, należy wprowadzić pełną ścieżkę do pliku lub zarówno sumę kontrolną, jak i ścieżkę.

Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, poczynszyszy od `\\`, a nie od litery dysku. Na przykład: `\\server\shared_folder\file.exe`. Jeśli ścieżka do pliku zawiera literę dysku sieciowego, możesz uzyskać błąd *Nie odnaleziono pliku*.

11. Kliknij przycisk **Zapisz**.
12. Zaznacz pole obok zadania.
13. Kliknij przycisk **Uruchom**.

W rezultacie Kaspersky Endpoint Security tworzy kopię pliku i przenosi tę kopię do Kwarantanny. Plik możesz pobrać z Kwarantanny w Web Console.

Usuń plik

Możesz zdalnie usunąć pliki przy użyciu zadania *Usuń plik*. Na przykład, podczas reagowania na zagrożenie możesz zdalnie usunąć plik.

Możesz skonfigurować ustawienia tylko w Web Console.

*W celu utworzenia zadania *Usuń plik*:*

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

b. Na liście rozwijalnej **Typ zadania** wybierz **Usuń plik**.

c. W polu **Nazwa zadania** wpisz krótki opis.

d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij przycisk **Dalej**.

Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. Na liście plików kliknij **Dodaj**.

Zostanie uruchomiony kreator dodawania plików.

10. Aby dodać plik, należy wprowadzić pełną ścieżkę do pliku lub zarówno sumę kontrolną, jak i ścieżkę.

Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, począwszy od `\\`, a nie od litery dysku. Na przykład: `\\server\shared_folder\file.exe`. Jeśli ścieżka do pliku zawiera literę dysku sieciowego, możesz uzyskać błąd *Nie odnaleziono pliku*.

11. Kliknij przycisk **Zapisz**.

12. Zaznacz pole obok zadania.

13. Kliknij przycisk **Uruchom**.

W rezultacie, Kaspersky Endpoint Security usunie plik z komputera. Jeśli plik jest zablokowany przez inny proces, zadanie jest wyświetlany jako *Zakończona*, ale sam plik jest usuwany tylko po ponownym uruchomieniu komputera. Po ponownym uruchomieniu komputera potwierdź usunięcie pliku.

Zadanie *Usuń plik* może zostać zakończone błędem *Dostęp zabroniony*, jeśli próbujesz usunąć plik wykonywalny, który jest aktualnie uruchomiony. [Utwórz zadanie kończenia procesu](#) dla pliku i spróbuj ponownie.

Rozpoczęcie procesu

Możesz zdalnie uruchomić pliki przy użyciu zadania *Rozpoczęcie procesu*. Na przykład, możesz zdalnie uruchomić narzędzie, które tworzy plik konfiguracyjny komputera. Następnie możesz użyć [zadania Uzyskaj plik](#), aby otrzymać utworzony plik w konsoli Kaspersky Security Center Web Console.

Możesz skonfigurować ustawienia tylko w Web Console.

W celu utworzenia zadania Rozpoczęcie procesu:

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

Zostanie otwarta lista zadań.

2. Kliknij przycisk **Dodaj**.

Zostanie uruchomiony Kreator tworzenia zadania.

3. Skonfiguruj ustawienia zadania:

a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.

b. Na liście rozwijalnej **Typ zadania** wybierz **Rozpoczęcie procesu**.

c. W polu **Nazwa zadania** wpisz krótki opis.

d. W sekcji **Wybierz urządzenia, do których zadanie zostanie przypisane** wybierz obszar zadania.

4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij przycisk **Dalej**.

Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

8. Zostanie otwarte okno właściwości zadania.

9. Wybierz zakładkę **Ustawienia aplikacji**.

10. Wpisz polecenie rozpoczęcia procesu.

Na przykład, jeśli chcesz uruchomić narzędzie (`utility.exe`), które zapisuje informacje o konfiguracji komputera do pliku `conf.txt`, musi wprowadzić następujące wartości:

- **Polecenie wykonywalne** – `utility.exe`

- **Argumenty wiersza polecenia** – /R conf.txt
- **Ścieżka do folderu roboczego** – C:\Users\admin\Diagnostic\

Alternatywnie, w polu **Polecenie wykonywalne** możesz wprowadzić C:\Users\admin\Diagnostic\utility.exe /R conf.txt. W tym przypadku nie musisz wprowadzać reszty ustawień.

11. Kliknij przycisk **Zapisz**.
12. Zaznacz pole obok zadania.
13. Kliknij przycisk **Uruchom**.

Kaspersky Endpoint Security uruchomi polecenie w trybie cichym i uruchomi proces. Możesz przejrzeć wyniki zadania we właściwościach zadania, w sekcji **Wyniki**.

Kończenie działania procesu

Możesz zdalnie zakończyć działanie procesu, korzystając z zadania *Kończenie działania procesu*. Na przykład, możesz zdalnie zakończyć działanie narzędzia testującego prędkość internetu, które zostało uruchomione przy użyciu [zadania *Rozpoczęcie procesu*](#).

Jeśli chcesz zapobiec uruchomieniu pliku, możesz skonfigurować [komponent *Zapobieganie wykonywaniu*](#). Możesz zabronić wykonaniu plików wykonywalnych, skryptów, plików formatów office.

Zadanie *Zakończ proces* posiada następujące ograniczenia:

- Procesy Krytycznego obiektu systemowego (SCO) nie mogą zostać zakończone. Krytyczne obiekty systemowe to pliki, które są wymagane przez system operacyjny i aplikację Kaspersky Endpoint Security for Windows do działania.
- Możesz skonfigurować zadanie dla EDR Optimum w Web Console i Cloud Console. Ustawienia zadania dla EDR Expert są dostępne tylko w Cloud Console.

W celu utworzenia zadania *Kończenie działania procesu*:

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zadania**.
Zostanie otwarta lista zadań.
2. Kliknij przycisk **Dodaj**.
Zostanie uruchomiony Kreator tworzenia zadania.
3. Skonfiguruj ustawienia zadania:
 - a. Na liście rozwijalnej **Aplikacja** wybierz **Kaspersky Endpoint Security for Windows (11.7.0)**.
 - b. Na liście rozwijanej **Typ zadania** wybierz **Działanie procesu zostało zakończone**.
 - c. W polu **Nazwa zadania** wpisz krótki opis.
 - d. W sekcji **Wybierz urządzenia, do których zostanie przypisane zadanie** wybierz obszar zadania.
4. Wybierz urządzenia zgodnie z opcją wybranego obszaru zadania. Kliknij przycisk **Dalej**.

5. Wprowadź poświadczenia konta użytkownika, którego uprawnień chcesz użyć do uruchomienia zadania. Kliknij przycisk **Dalej**.

Domyślnie, Kaspersky Endpoint Security uruchamia zadanie jako konto użytkownika systemu (SYSTEM).

6. Zakończ działanie kreatora, klikając przycisk **Zakończ**.

Nowe zadanie zostanie wyświetlone na liście zadań.

7. Kliknij nowe zadanie.

Zostanie otwarte okno właściwości zadania.

8. Wybierz zakładkę **Ustawienia aplikacji**.

9. Aby zakończyć proces, musisz wybrać plik, którego działanie chcesz zakończyć. Możesz wybrać plik na jeden z następujących sposobów:

- Wprowadź pełną nazwę pliku.
- Wprowadź skrót pliku i ścieżkę do pliku.
- Wprowadź PID procesu (dotyczy tylko zadań lokalnych).

Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, poczynawszy od `\\`, a nie od litery dysku. Na przykład: `\\server\shared_folder\file.exe`. Jeśli ścieżka do pliku zawiera literę dysku sieciowego, możesz uzyskać błąd *Nie odnaleziono pliku*.

10. W oknie właściwości zadania wybierz zakładkę **Terminarz**.

11. Skonfiguruj terminarz zadania.

Wake-on-LAN nie jest dostępne dla tego zadania. Upewnij się, że komputer jest włączony do uruchomienia zadania.

12. Kliknij przycisk **Zapisz**.

13. Zaznacz pole obok zadania.

14. Kliknij przycisk **Uruchom**.

W rezultacie, Kaspersky Endpoint Security zakończy proces na komputerze. Na przykład, jeśli aplikacja 'GRA' jest uruchomiona i zakończy proces `game.exe`, aplikacja zostanie zamknięta bez zapisywania danych. Możesz przejrzeć wyniki zadania we właściwościach zadania, w sekcji **Wyniki**.

Zapobieganie wykonywaniu

Zapobieganie wykonywaniu umożliwia zarządzanie uruchamianiem plików wykonywalnych i skryptów, a także otwieraniem plików formatu office. W ten sposób możesz, na przykład, zapobiec wykonaniu aplikacji, które uważasz za niezabezpieczone. Zapobieganie wykonywaniu obsługuje [zestaw rozszerzeń plików pakietu office](#) oraz [zestaw interpreterów skryptu](#).

Reguła zapobiegania wykonywaniu

Zapobieganie wykonywaniu zarządza dostępem użytkownika do plików z regułami zapobiegania wykonywaniu. *Reguły zapobiegania wykonywaniu* to zestaw kryteriów, które są uznawane podczas blokowania. Aplikacja identyfikuje pliki według ich ścieżek lub sum kontrolnych wyliczonych przy użyciu algorytmów haszowania MD5 i SHA256.

Możesz utworzyć reguły Zapobiegania wykonywaniu:

- W szczegółach wykrycia.

Szczegóły wykrycia to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu i zarządzaniu działaniami odpowiedzi. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do [Kaspersky Endpoint Detection and Response Optimum](#).

- Korzystając z zasad grupy lub lokalnych ustawień aplikacji.

Musisz wprowadzić ścieżkę do pliku lub sumę kontrolną pliku (SHA256 lub MD5), albo obie te wartości.

Możesz także zarządzać Zapobieganiem wykonywaniu lokalnie przy użyciu [wiersza polecenia](#).

Nie jest zalecane utworzenie więcej niż 5 000 reguł zapobiegania uruchomieniu, gdyż może to spowodować niestabilność systemu.

Reguły zapobiegania nie obejmują plików na płytach CD lub obrazów ISO. Aplikacja nie blokuje wykonywania lub otwierania tych plików.

Tryby reguły zapobiegania wykonywaniu

Komponent Zapobieganie wykonywaniu może działać w dwóch trybach:

- **Tylko statystyki.**

W tym trybie Kaspersky Endpoint Security publikuje zdarzenie dotyczące prób uruchomienia obiektów wykonywalnych lub otwarcia dokumentów, które odpowiadają kryteriom reguły blokowania, w Dzienniku zdarzeń Windows oraz w Kaspersky Security Center, ale nie blokują próby uruchomienia lub otwarcia obiektu lub dokumentu. Ten tryb jest wybrany domyślnie.

- **Aktywny.**

W tym trybie aplikacja blokuje wykonanie obiektów lub otwieranie dokumentów, które odpowiadają kryteriom reguły blokowania. Aplikacja publikuje także zdarzenie dotyczące prób wykonania obiektów lub otwarcia dokumentów w Dzienniku zdarzeń Windows oraz dzienniku zdarzeń Kaspersky Security Center.

Zarządzanie zapobieganiem wykonaniu

Możesz skonfigurować ustawienia komponentu tylko w Web Console.

W celu zapobiegania wykonywaniu:

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Wybierz **Detection and Response** → **Endpoint Detection and Response**.

5. Użyj przełącznika **Zapobieganie wykonywaniu**, aby włączyć lub wyłączyć komponent.

6. W sekcji **Akcja podczas wykonywania lub otwierania zabronionego obiektu** wybierz tryb działania komponentu:

- **Blokuj i zapisz do raportu.** W tym trybie aplikacja blokuje wykonanie obiektów lub otwieranie dokumentów, które odpowiadają kryteriom reguły blokowania. Aplikacja publikuje także zdarzenie dotyczące prób wykonania obiektów lub otwarcia dokumentów w Dzienniku zdarzeń Windows oraz dzienniku zdarzeń Kaspersky Security Center.
- **Tylko zapisuj zdarzenia.** W tym trybie Kaspersky Endpoint Security publikuje zdarzenie dotyczące prób uruchomienia obiektów wykonywalnych lub otwarcia dokumentów, które odpowiadają kryteriom reguły blokowania, w Dzienniku zdarzeń Windows oraz w Kaspersky Security Center, ale nie blokują próby uruchomienia lub otwarcia obiektu lub dokumentu. Ten tryb jest wybrany domyślnie.

7. Utwórz listę reguł zapobiegania wykonywaniu:

a. Kliknij przycisk **Dodaj**.

b. To spowoduje otwarcie okna; w tym oknie wprowadź nazwę reguły zapobiegania wykonywaniu (na przykład, *Aplikacja A*).

c. Z listy rozwijalnej **Typ** wybierz obiekt, który chcesz zablokować: **Plik wykonywalny, Skrypt, Dokument Microsoft Office**.

Jeśli wybrałeś zły typ obiektu, Kaspersky Endpoint Security nie blokuje pliku lub skryptu.

d. Aby dodać plik, należy wprowadzić sumę kontrolną pliku (SHA256 lub MD5), pełną ścieżkę do pliku lub sumę kontrolną i ścieżkę.

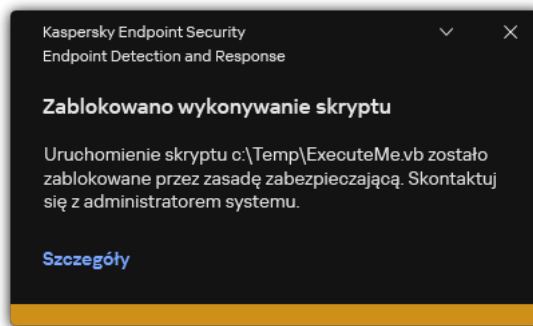
Jeśli plik znajduje się na dysku sieciowym, wprowadź ścieżkę do pliku, począwszy od `\\`, a nie od litery dysku. Na przykład: `\\server\shared_folder\file.exe`. Jeśli ścieżka dostępu do pliku zawiera literę dysku sieciowego, Kaspersky Endpoint Security nie blokuje pliku lub skryptu.

Zapobieganie wykonywaniu obsługuje [zestaw rozszerzeń plików pakietu office](#) oraz [zestaw interpreterów skryptu](#).

e. Kliknij **OK**.

8. Zapisz swoje zmiany.

W rezultacie Kaspersky Endpoint Security zablokuje wykonanie obiektów: uruchomienie skryptów i plików wykonywalnych, otwarcie plików formatów office. Jednakże możesz, na przykład, otworzyć plik skryptu w edytorze tekstu nawet wtedy, gdy uruchomienie skryptów zostanie uniemożliwione. Podczas blokowania wykonania obiektu Kaspersky Endpoint Security wyświetli standardowe powiadomienie (patrz rysunek poniżej), jeśli powiadomienia [są włączone w ustawieniach aplikacji](#).



Powiadomienie o zapobieganiu wykonywania

Izolacja sieci komputerowej

Izolacja sieci komputerowej umożliwia automatyczne izolowanie komputera od sieci w odpowiedzi na wykrycie wskaźnika naruszeń bezpieczeństwa (IOC).

Jeśli Izolacja sieci jest włączona, aplikacja zrywa wszystkie aktywne połączenia i blokuje wszystkie nowe połączenia sieciowe TCP/IP na komputerze, za wyjątkiem następujących połączeń:

- Połączenia znajdujące się w wykluczeniach Izolacji sieci.
- Połączenia zainicjowane przez usługi Kaspersky Endpoint Security.
- Połączenia zainicjowane przez agenta administracji Kaspersky Security Center.

Zarządzanie Izolacją sieci

Możesz skonfigurować ustawienia komponentu tylko w Web Console.

Możesz skonfigurować Izolację sieci tak, aby była włączana automatycznie w odpowiedzi na wykrycie IOC. Możesz także ręcznie włączyć i wyłączyć Izolację sieci.

Izolację sieci można włączyć:

- W szczegółach wykrycia.
Szczegóły wykrycia to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu i zarządzaniu działaniami odpowiedzi. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do [Kaspersky Endpoint Detection and Response Optimum](#).
- Przy pomocy lokalnych ustawień aplikacji.

[Konfigurowanie Izolacji sieci tak, aby była włączana automatycznie w odpowiedzi na wykrycie IOC](#)

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

Zostanie otwarta lista zadań.

2. Wybierz zadanie **Skanowanie IOC** programu Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości zadania.

Jeśli to konieczne, utwórz zadanie [Skanowanie IOC](#).

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. W sekcji **Akcja po wykryciu IOC** zaznacz pola **Podejmij działania w odpowiedzi po znalezieniu IOC** i **Odizoluj komputer od sieci**.

5. Zapisz swoje zmiany.

W wyniku tego działania, po wykryciu IOC, aplikacja odizoluje komputer od sieci, aby zapobiec rozprzestrzenianiu zagrożenia.

[Ręczne włączenie Izolacji sieci komputera](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.

2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.

Spowoduje to otwarcie właściwości komputera.

3. Wybierz zakładkę **Aplikacje**.

4. Kliknij **Kaspersky Endpoint Security for Windows**.

Spowoduje to otwarcie lokalnych ustawień aplikacji.

5. Wybierz zakładkę **Ustawienia aplikacji**.

6. Wybierz **Detection and Response** → **Endpoint Detection and Response**.

7. W sekcji **Izolacja sieci** kliknij **Odizoluj komputer od sieci**.

8. Zapisz swoje zmiany.

Możesz skonfigurować Izolację sieci tak, aby była wyłączana automatycznie po upływie określonego czasu. Domyślnie, aplikacja wyłącza Izolację sieci po 5 godzinach od czasu, gdy została włączona. Możesz także ręcznie wyłączyć Izolację sieci. Po wyłączeniu Izolacji sieci komputer może używać sieci bez ograniczeń.

[Konfigurowanie opóźnienia automatycznego wyłączenia Izolacji sieci dla komputera](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Detection and Response** → **Endpoint Detection and Response**.
5. W sekcji **Izolacja sieci** kliknij **Skonfiguruj ustawienia odblokowania komputera**.
6. To spowoduje otwarcie okna; w tym oknie zaznacz pole **Automatycznie odblokuj izolowany komputer w ciągu N godzin** i wprowadź opóźnienie automatycznego wyłączenia Izolacji sieci.
7. Zapisz swoje zmiany.

Ręczne wyłączenie Izolacji sieci komputera

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zarządzane urządzenia**.
2. Wybierz komputer, dla którego chcesz skonfigurować lokalne ustawienia aplikacji.
Spowoduje to otwarcie właściwości komputera.
3. Wybierz zakładkę **Aplikacje**.
4. Kliknij **Kaspersky Endpoint Security for Windows**.
Spowoduje to otwarcie lokalnych ustawień aplikacji.
5. Wybierz zakładkę **Ustawienia aplikacji**.
6. Wybierz **Detection and Response** → **Endpoint Detection and Response**.
7. W sekcji **Izolacja sieci** kliknij **Odblokuj komputer odizolowany od sieci**.
8. Zapisz swoje zmiany.

Możesz także wyłączyć Izolację sieci lokalnie przy użyciu [wiersza polecenia](#).

Wykluczenia Izolacji sieci

Możesz skonfigurować wykluczenia Izolacji sieci. Połączenia sieciowe, które odpowiadają regułom, nie są blokowane na komputerze, gdy Izolacja sieci jest włączona.

Aby skonfigurować wykluczenia izolacji sieci, możesz użyć listy *standardowych profili sieciowych*. Domyślnie, wykluczenia obejmują profile sieciowe zawierające reguły, które zapewniają nieprzerwane działanie urządzeń z rolami serwera DNS/DHCP i klienta DNS/DHCP. Możesz także ręcznie zmodyfikować ustawienia standardowych profili sieciowych lub zdefiniować wykluczenia (patrz instrukcja poniżej).

Wykluczenia określone we właściwościach zasady są stosowane tylko wtedy, gdy Izolacja sieci zostaje włączona automatycznie w odpowiedzi na wykryte zagrożenie. Wykluczenia określone we właściwościach komputera są stosowane tylko wtedy, gdy Izolacja sieci zostanie włączona ręcznie we właściwościach komputera w konsoli Kaspersky Security Center.

Aktywna zasada nie zapobiega stosowaniu wykluczeń z Izolacji sieci, skonfigurowanej we właściwościach komputera, ponieważ te parametry mają inne scenariusze korzystania.

Dodawanie wykluczenia Izolacji sieci

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Detection and Response** → **Endpoint Detection and Response**.
5. W sekcji **Wykluczenia izolacji sieci** kliknij **Wykluczenia**.
6. To spowoduje otwarcie okna; w tym oknie kliknij **Dodaj z profilu** i wybierz standardowe profile sieciowe do konfigurowania wykluczeń.
Wykluczenia Izolacji sieci z profilu są dodawane do listy wykluczeń Izolacji sieci. Możesz przejrzeć właściwości połączenia sieciowego. Jeśli to konieczne, możesz zmodyfikować ustawienia połączenia sieciowego.
7. Jeśli to konieczne, ręcznie dodaj wykluczenie Izolacji sieci. Aby to zrobić, w oknie z listą wykluczeń kliknij **Dodaj** i ręcznie edytuj ustawienia połączenia sieciowego.
8. Zapisz swoje zmiany.

Możesz także przejrzeć listę wykluczenia Izolacji sieci lokalnie, korzystając z [wiersza polecenia](#).

Kaspersky Sandbox



Kaspersky Endpoint Security 11.7.0 teraz zawiera komponent Kaspersky Sandbox. Komponent umożliwia współdziałanie z rozwiązaniem Kaspersky Sandbox. *Rozwiązanie Kaspersky Sandbox* wykrywa i automatycznie blokuje zaawansowane zagrożenia na komputerach. Kaspersky Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Kaspersky Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Kaspersky Sandbox). Więcej informacji o rozwiązaniu można znaleźć w *pomocy dla* [Kaspersky Sandbox](#).

Podczas interakcji z Kaspersky Sandbox aplikacja umożliwia:

- Dodanie certyfikatu TLS dla bezpiecznego połączenia z serwerami Kaspersky Sandbox.

- Dodanie serwerów Kaspersky Sandbox.
- Wybranie środków reakcji na zagrożenie.
- Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (IOC).

Kaspersky Sandbox wymaga Kaspersky Security Center w wersji 13.2. Wcześniejsze wersje Kaspersky Security Center nie pozwalają na utworzenie autonomicznych zadań Skanowanie IOC w celu reakcji na zagrożenia.

Komponent może być zarządzany tylko przy użyciu konsoli Web Console. Nie możesz zarządzać tym komponentem przy użyciu Konsoli administracyjnej (MMC).

Integracja z Kaspersky Sandbox

Integracja z Kaspersky Sandbox obejmuje następujące kroki:

1 Instalowanie komponentu Kaspersky Sandbox

Możesz wybrać komponent Kaspersky Sandbox podczas [instalacji](#) lub [aktualizacji](#), a także przy użyciu zadania [Zmiana składników aplikacji](#).

Po wykonaniu zadania *Zmiana składników aplikacji* stan zadania zostanie wyświetlony niepoprawnie. Zamiast *Zakończono pomyślnie* zadanie posiada stan *Zaplanowane*. Jednakże zadanie może nadal zostać zakończone pomyślnie. Upewnij się, że nowy składnik został zainstalowany we właściwościach komputera konsoli Kaspersky Security Center (**Aplikacje** → **Kaspersky Endpoint Security for Windows** → **Components**) lub w lokalnym interfejsie aplikacji.

2 Dodawanie certyfikatu TLS

Aby skonfigurować zaufane połączenie z serwerami Kaspersky Sandbox, musisz przygotować certyfikat TLS. Następnie musisz dodać certyfikat do serwerów Kaspersky Sandbox i zasady Kaspersky Endpoint Security. Więcej informacji na temat przygotowywania certyfikatu i dodawania certyfikatu do serwerów znajdziesz w pomocy dla Kaspersky Sandbox.

[Jak dodać certyfikat TLS przy użyciu konsoli Web Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.

2. Kliknij nazwę zasady Kaspersky Endpoint Security.

Zostanie otwarte okno właściwości profilu.

3. Wybierz zakładkę **Ustawienia aplikacji**.

4. Przejdź do **Detection and Response** → **Kaspersky Sandbox**.

5. Kliknij **Ustawienia połączenia z serwerem**.

To spowoduje otwarcie okna ustawień połączenia z serwerem Kaspersky Sandbox.

6. W sekcji **Certyfikat serwera TLS** kliknij **Dodaj** i wybierz plik certyfikatu TLS.

Kaspersky Endpoint Security może mieć tylko jeden certyfikat TLS dla serwera Kaspersky Sandbox. Jeśli wcześniej dodałeś certyfikat TLS, ten certyfikat zostanie odwołany. Używany jest tylko ostatnio dodany certyfikat.

7. Skonfiguruj zaawansowane ustawienia połączeń dla serwerów Kaspersky Sandbox:

- **Przekroczono czas żądania.** Limit czasu połączenia dla serwera Kaspersky Sandbox został przekroczony. Po skonfigurowaniu upłygnięcia określonej ilości czasu, Kaspersky Endpoint Security wyśle żądanie do następnego serwera. Możesz zwiększyć limit czasu połączenia dla Kaspersky Sandbox, jeśli prędkość Twojego połączenia spada lub jeśli połączenie jest niestabilne. Domyślnie wynosi on 5 sekund.
- **Kolejka żądań Kaspersky Sandbox.** Rozmiar folderu kolejki żądań. Jeśli na komputerze jest dostęp do obiektu (uruchomiony plik wykonywalny lub otwarty dokument, na przykład w formacie DOCX lub PDF), Kaspersky Endpoint Security może także wysłać obiekt do skanowania wykonywanego przez Kaspersky Sandbox. Jeśli istnieje kilka żądań, Kaspersky Endpoint Security tworzy kolejkę żądań. Domyślnie, rozmiar folderu kolejki żądań jest ograniczony do 100 MB. Po osiągnięciu maksymalnego rozmiaru, Kaspersky Sandbox przestanie dodawać nowe żądania do kolejki i wyśle odpowiednie zdarzenie do Kaspersky Security Center. Możesz skonfigurować rozmiar folderu kolejki żądań w zależności od konfiguracji Twojego serwera.

8. Zapisz swoje zmiany.

W wyniku tego program Kaspersky Endpoint Security będzie sprawdzał certyfikat TLS. Jeśli certyfikat zostanie pomyślnie zweryfikowany, Kaspersky Endpoint Security wczyta plik certyfikatu do komputera podczas kolejnej synchronizacji z Kaspersky Security Center. Jeśli dodałeś dwa certyfikaty TLS, Kaspersky Sandbox użyje najnowszego certyfikatu do nawiązania zaufanego połączenia.

Możesz także dodać certyfikat TLS do komputera lokalnie przy użyciu [wiersza polecenia](#).

3 Włączanie komponentu Kaspersky Sandbox

Możesz włączyć lub wyłączyć komponent w ustawieniach zasady Kaspersky Endpoint Security for Windows.

W celu użycia komponentu spełnione muszą być następujące warunki:

- Aplikacja jest aktywowana, a funkcjonalność jest objęta licencją.
- Komponent Kaspersky Sandbox jest włączony.

[Jak włączyć lub wyłączyć Kaspersky Sandbox przy użyciu Web Console?](#) 

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Detection and Response** → **Kaspersky Sandbox**.
5. Użyj przełącznika **Integracja z Kaspersky Sandbox**, aby włączyć lub wyłączyć komponent.
6. Zapisz swoje zmiany.

Możesz także włączyć lub wyłączyć Kaspersky Sandbox lokalnie przy użyciu [wiersza polecenia](#).

W rezultacie komponent Kaspersky Sandbox jest włączony. Sprawdź stan działania komponentu, przeglądając *Raport dotyczący stanu komponentów aplikacji*. Stan działania komponentu można sprawdzić także w raportach, w lokalnym interfejsie Kaspersky Endpoint Security. Komponent **Kaspersky Sandbox** zostanie dodany do listy komponentów Kaspersky Endpoint Security.

4 Podłączanie komputerów do serwerów Kaspersky Sandbox

Aby podłączyć komputery do serwerów Kaspersky Sandbox z obrazami wirtualnymi systemów operacyjnych, musisz wprowadzić port i adres serwera. Więcej informacji dotyczących wdrożenia obrazów wirtualnych i skonfigurowania serwerów Kaspersky Sandbox można znaleźć w pomocy dla [Kaspersky Sandbox](#).

[Jak podłączyć komputery do serwerów Kaspersky Sandbox przy użyciu Web Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Przejdź do **Detection and Response** → **Kaspersky Sandbox**.
5. W sekcji **Serwery Kaspersky Sandbox** kliknij **Dodaj**.
6. To okno zostanie otwarte; w tym oknie wprowadź port i adres serwera Kaspersky Sandbox (IPv4, IPv6, DNS).
7. Zapisz swoje zmiany.

5 Nawiązywanie połączenia w tle między Kaspersky Security Center Web Console a Serwerem administracyjnym

Aby rozwiązanie Kaspersky Sandbox działało z Serwerem administracyjnym poprzez Kaspersky Security Center Web Console, należy nawiązać nowe bezpieczne połączenie – *połączenie w tle*. Więcej informacji o integracji Kaspersky Security Center z innymi rozwiązaniami Kaspersky można znaleźć w [pomocy dla Kaspersky Security Center](#).

[Nawiązywanie połączenia w tle w Web Console](#)

1. W oknie głównym Web Console wybierz **Ustawienia konsoli** → **Integracja**.
2. Przejdź do sekcji **Integracja między usługami**.
3. Przesuń przełącznik **Nawiąż połączenie w tle dla integracji między usługami**.
4. Zapisz swoje zmiany.

Jeśli połączenie w tle między Kaspersky Security Center Web Console a Serwerem administracyjnym nie zostanie nawiązane, autonomiczne zadania skanowania IOC nie może zostać utworzone jako część Threat Response.

6 Włączanie przesyłania danych do Serwera administracyjnego

Aby użyć wszystkich funkcji Kaspersky Sandbox, upewnij się, że przesyłanie danych pliku poddanego kwarantannie jest włączone. Dane są wymagane do uzyskania informacji o plikach poddanych kwarantannie na komputerze za pośrednictwem Web Console. Na przykład, możesz pobrać plik z kwarantanny do analizy w Web Console.

[Jak włączyć przesyłanie danych do Serwera administracyjnego w Web Console?](#)

1. W oknie głównym Web Console wybierz **Urządzenia** → **Zasady i profile**.
2. Kliknij nazwę zasady Kaspersky Endpoint Security.
Zostanie otwarte okno właściwości profilu.
3. Wybierz zakładkę **Ustawienia aplikacji**.
4. Wybierz **Ustawienia główne** → **Raporty i pliki danych**.
5. W sekcji **Przesyłanie danych do Serwera administracyjnego** zaznacz pole **Informacje o plikach poddanych kwarantannie**.
6. Zapisz swoje zmiany.

Migracja z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows

Jeśli używasz Kaspersky Endpoint Security 11.7.0 lub nowszej wersji z zainstalowanym komponentem Kaspersky Sandbox, od razu po instalacji możliwe jest pełne współdziałanie z rozwiązaniem Kaspersky Sandbox. Komponent Kaspersky Sandbox nie jest kompatybilny z Kaspersky Endpoint Agent. Jeśli Kaspersky Endpoint Agent jest zainstalowany na komputerze, po zaktualizowaniu Kaspersky Endpoint Security do wersji 11.7.0, Kaspersky Sandbox nadal działa z Kaspersky Endpoint Security. Dodatkowo, Kaspersky Endpoint Agent zostanie usunięty z komputera. Aby zakończyć migrację z Kaspersky Endpoint Agent do Kaspersky Endpoint Security for Windows, musisz przenieść ustawienia zasady i zadania przy pomocy [Kreatora migracji](#).

Jeśli używasz Kaspersky Endpoint Security 11.4.0–11.6.0 do współdziałania z Kaspersky Sandbox, aplikacja zawiera Kaspersky Endpoint Agent. Możesz zainstalować Kaspersky Endpoint Agent wraz z Kaspersky Endpoint Security.

Komponent Kaspersky Sandbox, który jest częścią Kaspersky Endpoint Security, obsługuje współdziałanie z rozwiązaniem Kaspersky Sandbox w wersji 2.0. Rozwiązanie Kaspersky Sandbox w wersji 1.0 nie jest obsługiwane.

Zarządzanie aplikacją z poziomu wiersza poleceń

Możesz zarządzać Kaspersky Endpoint Security z poziomu wiersza poleceń. Możesz wyświetlić listę poleceń do zarządzania aplikacją, wykonując polecenie `HELP`. Aby zapoznać się z informacjami o składni konkretnego polecenia, wpisz `HELP <polecenie>`.

Znaki specjalne w poleceniu muszą zostać pominięte. Aby pominąć znaki `&`, `|`, `(`, `)`, `<`, `>`, `^`, użyj znaku `^` (na przykład, aby użyć znaku `&`, wprowadź `^&`). Aby pominąć znak `%`, wprowadź `%%`.

Instalowanie aplikacji

Kaspersky Endpoint Security może zostać zainstalowany z poziomu wiersza poleceń w jednym z następujących trybów:

- W trybie interaktywnym, korzystając z Kreatora instalacji aplikacji.
- W trybie cichym. W tym trybie nie jest wymagany udział w procesie instalacji. Aby zainstalować aplikację w trybie cichym, użyj przełączników `/s` i `/qn`.

Przed zainstalowaniem aplikacji w trybie cichym należy otworzyć i przeczytać Umowę licencyjną i Politykę prywatności. Umowa licencyjna oraz Polityka prywatności znajdują się w [pakiecie dystrybucyjnym Kaspersky Endpoint Security](#). Przejście do instalacji aplikacji jest możliwe tylko wtedy, gdy w pełni przeczytałeś, zrozumiałeś i zaakceptowałeś warunki Umowy licencyjnej, przeczytałeś i zrozumiałeś, że Twoje dane będą przetwarzane i przesyłane (w tym do innych krajów) zgodnie z Polityką prywatności oraz w pełni przeczytałeś i zrozumiałeś Politykę prywatności. Jeśli nie akceptujesz warunków i postanowień Umowy licencyjnej i Polityki prywatności, nie instaluj ani nie używaj Kaspersky Endpoint Security.

W celu zainstalowania aplikacji lub zaktualizowania poprzedniej wersji aplikacji:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się pakiet dystrybucyjny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<nazwa użytkownika>
/pKLPASSWD=<hasło> /pKLPASSWDAREA=<zakres działania hasła>] [/pENABLETRACES=1|0
/pTRACESLEVEL=<poziom śledzenia>] [/s]
```

LUB

```
msiexec /i <nazwa pakietu dystrybucyjnego> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<nazwa użytkownika> KLPASSWD=<hasło>
KLPASSWDAREA=<zakres działania hasła>] [ENABLETRACES=1|0 TRACESLEVEL=<poziom
śledzenia>] [/qn]
```

EULA=1	Akceptacja lub odrzucenie warunków Umowy licencyjnej. Umowa licencyjna jest zawarta w pakiecie dystrybucyjnym Kaspersky Endpoint Security .
--------	---

	<p>Akceptacja warunków Umowy licencyjnej jest niezbędna do zainstalowania aplikacji lub jej aktualizacji.</p>
PRIVACYPOLICY=1	<p>Akceptacja Polityki prywatności. Treść Polityki prywatności znajduje się w pakiecie dystrybucyjnym Kaspersky Endpoint Security.</p> <p>Aby zainstalować aplikację lub zaktualizować wersję aplikacji, musisz zaakceptować Politykę prywatności.</p>
KSN	<p>Akceptacja lub odmowa uczestnictwa w Kaspersky Security Network. Jeśli nie ustawiono wartości dla tego parametru, Kaspersky Endpoint Security wyświetli monit o potwierdzenie zgody lub odmowę uczestniczenia w KSN przy pierwszym uruchomieniu Kaspersky Endpoint Security. Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – zgoda na uczestniczenie w KSN. • 0 – odmowa uczestniczenia w KSN (wartość domyślna). <p>Pakiet dystrybucyjny Kaspersky Endpoint Security jest zoptymalizowany do użycia z Kaspersky Security Network. Jeśli zdecydowałeś się nie uczestniczyć w Kaspersky Security Network, powinieneś zaktualizować Kaspersky Endpoint Security od razu po zakończeniu instalacji.</p>
ALLOWREBOOT=1	<p>Automatyczne ponowne uruchamianie komputera, jeśli jest wymagane po zainstalowaniu lub zaktualizowaniu aplikacji. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość, automatyczne ponowne uruchomienie komputera zostanie zablokowane.</p> <p>Ponowne uruchomienie nie jest wymagane podczas instalowania Kaspersky Endpoint Security. Ponowne uruchomienie jest wymagane tylko wtedy, gdy przed instalacją musisz usunąć niekompatybilne aplikacje. Ponowne uruchomienie może być też wymagane podczas aktualizowania wersji aplikacji.</p>
SKIPPRODUCTCHECK=1	<p>Wyłączenie sprawdzania niekompatybilnego oprogramowania. Lista niekompatybilnego oprogramowania jest dostępna w pliku incompatible.txt, który znajduje się w pakiecie dystrybucyjnym. Jeśli dla tego parametru nie zostanie ustawiona żadna wartość i zostanie wykryte niekompatybilne oprogramowanie, instalacja Kaspersky Endpoint Security zostanie zakończona.</p>
SKIPPRODUCTUNINSTALL=1	<p>Wyłączenie automatycznego usuwania wykrytego niekompatybilnego oprogramowania. Jeśli dla tego parametru nie zostanie ustawiona wartość, Kaspersky Endpoint Security spróbuje usunąć niekompatybilne oprogramowanie.</p> <p>Automatyczne usuwanie niekompatybilnego oprogramowania nie może być włączone podczas instalacji Kaspersky Endpoint Security za pomocą instalatora msiexec. Użyj setup_ks.exe, aby włączyć automatyczne usuwanie niekompatybilnego oprogramowania.</p>
KLLOGIN	<p>Ustaw nazwę użytkownika, aby uzyskać dostęp do funkcji i ustawień</p>

	Kaspersky Endpoint Security (komponent Ochrona hasłem). Nazwa użytkownika jest ustawiana wraz z parametrami KLPASSWD i KLPASSWDAREA. Nazwa użytkownika KLAdmin jest używana domyślnie.
KLPASSWD	Określ hasło dostępu do funkcji i ustawień Kaspersky Endpoint Security (hasło jest określane wraz z parametrami KLLOGIN i KLPASSWDAREA). Jeśli określiłeś hasło, ale nie określiłeś nazwy użytkownika z parametrem KLLOGIN, domyślnie używana będzie nazwa użytkownika KLAdmin.
KLPASSWDAREA	Zakres działania hasła dostępu do funkcji i ustawień Kaspersky Endpoint Security. Jeśli użytkownik spróbuje wykonać działanie, które znajduje się w tym obszarze, Kaspersky Endpoint Security wyświetli monit o podanie danych uwierzytelniających konta użytkownika (parametry KLLOGIN i KLPASSWD). Użyj znaku „;”, aby określić kilka wartości. Dostępne wartości: <ul style="list-style-type: none"> • SET – modyfikowanie ustawień aplikacji. • EXIT – zakończenie działania aplikacji. • DISPROTECT – wyłączanie komponentów ochrony i zatrzymywanie zadań skanowania. • DISPOLICY – wyłączanie zasady Kaspersky Security Center. • UNINST – usunięcie aplikacji z komputera. • DISCTRL – wyłączenie składników kontroli. • REMOVELIC – usuwanie klucza. • REPORTS – wyświetlanie raportów.
ENABLETRACES	Włączanie lub wyłączanie śledzenia aplikacji. Po uruchomieniu, program Kaspersky Endpoint Security zapisuje pliki śledzenia w folderze %ProgramData%\Kaspersky Lab\KES\Traces. Dostępne wartości: <ul style="list-style-type: none"> • 1 – śledzenie jest włączone. • 0 – śledzenie jest wyłączone (wartość domyślna).
TRACESLEVEL	Poziom szczegółowości śledzenia. Dostępne wartości: <ul style="list-style-type: none"> • 100 (krytyczny). Tylko wiadomości dotyczące błędów krytycznych. • 200 (wysoki). Wiadomości o wszystkich błędach, w tym błędach krytycznych. • 300 (diagnostyczny). Wiadomości o wszystkich błędach, a także ostrzeżenia. • 400 (ważny). Wszystkie wiadomości o błędach, ostrzeżenia i dodatkowe informacje. • 500 (normalny). Wiadomości o wszystkich błędach i ostrzeżeniach, a także szczegółowe informacje o działaniu aplikacji w trybie normalnym (domyślnie). • 600 (niski). Wszystkie wiadomości.

AMPPL	<p>Włącza lub wyłącza ochronę procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL (Antimalware Protected Process Light). Więcej informacji na temat technologii AM-PPL znajdziesz na stronie internetowej firmy Microsoft.</p> <p>Technologia AM-PPL jest dostępna dla systemu Windows 10 w wersji 1703 (RS2) lub nowszej oraz systemów operacyjnych Windows Server 2019.</p> <p>Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – ochrona procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest włączona. • 0 – ochrona procesów Kaspersky Endpoint Security przy użyciu technologii AM-PPL jest wyłączona.
RESTAPI	<p>Zarządzanie aplikacją za pośrednictwem interfejsu API REST. Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, należy podać nazwę użytkownika (parametr RESTAPI_User).</p> <p>Dostępne wartości:</p> <ul style="list-style-type: none"> • 1 – zarządzanie za pośrednictwem interfejsu API REST jest dozwolone. • 0 – zarządzanie za pośrednictwem interfejsu API REST jest zablokowane (wartość domyślna). <p>Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, zarządzanie przy użyciu systemów administracyjnych musi być dozwolone. W tym celu ustaw parametr AdminKitConnector=1. Jeśli zarządzasz aplikacją za pośrednictwem interfejsu API REST, zarządzanie aplikacją przy użyciu systemów administracyjnych firmy Kaspersky jest niemożliwe.</p>
RESTAPI_User	<p>Nazwa użytkownika konta domeny Windows używanego do zarządzania aplikacją za pośrednictwem interfejsu API REST. Zarządzanie aplikacją za pośrednictwem interfejsu API REST jest dostępne tylko dla tego użytkownika. Wpisz nazwę użytkownika w formacie <DOMAIN>\<UserName> (na przykład: RESTAPI_User=COMPANY\Administrator). Możesz wybrać tylko jednego użytkownika do pracy z interfejsem API REST.</p> <p>Dodanie nazwy użytkownika jest wymaganiem wstępnym zarządzania aplikacją za pośrednictwem interfejsu API REST.</p>
RESTAPI_Port	<p>Port używany do zarządzania aplikacją za pośrednictwem interfejsu API REST. Domyślnie używany jest port 6782.</p>
RESTAPI_Certificate	<p>Certyfikat do identyfikowania żądań (na przykład, RESTAPI_Certificate=C:\cert.pem). Bezpieczna interakcja Kaspersky Endpoint Security z klientem REST wymaga skonfigurowania identyfikacji żądania. W tym celu należy zainstalować certyfikat i podpisać ładunek każdego żądania.</p>
ADMINKITCONNECTOR	<p>Zarządzanie aplikacjami za pomocą systemów administracyjnych. Systemy administracyjne obejmują, na przykład, Kaspersky Security Center. Oprócz systemów administracyjnych Kaspersky możesz korzystać z rozwiązań innych firm. Kaspersky Endpoint Security oferuje w tym celu interfejs API.</p> <p>Dostępne wartości:</p>

- 1 – dozwolone jest zarządzanie aplikacjami za pomocą systemów administracyjnych (wartość domyślna).
- 0 – zarządzanie aplikacjami jest dozwolone tylko przez interfejs lokalny.

Na przykład:

```
setup_ks.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1  
/pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1  
KSN=1 KLLOGIN=Admin KLPASSWD=Password  
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_ks.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1  
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Po zainstalowaniu Kaspersky Endpoint Security licencja testowa zostanie aktywowana, chyba że nie dostarczyłeś kodu aktywacyjnego w [pliku setup.ini](#). Licencja testowa ma zazwyczaj krótki okres ważności. Po wygaśnięciu licencji testowej wszystkie funkcje programu Kaspersky Endpoint Security stają się niedostępne. Aby kontynuować korzystanie z aplikacji, należy aktywować aplikację z licencją komercyjną przy użyciu [Kreatora aktywacji aplikacji](#) lub [specjalnego polecenia](#).

Podczas instalacji aplikacji lub uaktualniania jej wersji w trybie cichym używane są następujące pliki:

- [setup.ini](#) – ustawienia ogólne dla instalacji aplikacji
- [install.cfg](#) – ustawienia działania Kaspersky Endpoint Security
- setup.reg – klucze rejestru

Klucze rejestru z pliku setup.reg zostają zapisane do rejestru tylko wtedy, gdy w [pliku setup.ini](#), dla parametru SetupReg ustawiono wartość setup.reg. Plik setup.reg jest generowany przez ekspertów z Kaspersky. Nie jest zalecane modyfikowanie zawartości tego pliku.

Aby zastosować ustawienia z plików setup.ini, install.cfg i setup.reg, umieść te pliki w folderze zawierającym pakiet dystrybucyjny Kaspersky Endpoint Security. Możesz także umieścić plik setup.reg w innym folderze. Jeśli to konieczne, musisz określić ścieżkę do pliku w następującym poleceniu instalacji aplikacji: SETUPREG=<ścieżka do pliku setup.reg>.

Aktywowanie aplikacji

W celu aktywowania programu z poziomu wiersza poleceń:

w wierszu poleceń wpisz następujące polecenie:

```
avp.com license /add <kod aktywacyjny lub plik klucza> [/login=<nazwa użytkownika>  
/password=<hasło>]
```

Jeśli [ochrona hasłem jest włączona](#) należy wprowadzić dane uwierzytelniające konta (/login=<nazwa użytkownika> /password=<hasło>).

Deinstalacja aplikacji

Kaspersky Endpoint Security może zostać odinstalowany z poziomu wiersza poleceń w jeden z następujących sposobów:

- W trybie interaktywnym, korzystając z Kreatora instalacji aplikacji.
- W trybie cichym. W tym trybie nie jest wymagany udział użytkownika w procesie deinstalacji. Aby odinstalować aplikację w trybie cichym, użyj przełączników /s i /qn.

W celu odinstalowania aplikacji w trybie cichym:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się pakiet dystrybucyjny Kaspersky Endpoint Security.
3. Uruchom następujące polecenie:
 - Jeśli proces deinstalacji nie jest [chroniony hasłem](#):
`setup_kes.exe /s /x`
LUB
`msiexec.exe /x <GUID> /qn`
<GUID> jest unikatowym identyfikatorem aplikacji. Możesz znaleźć identyfikator GUID aplikacji za pomocą następującego polecenia:
`wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber.`

- Jeśli proces deinstalacji jest [chroniony hasłem](#):
`setup_kes.exe /pKLLLOGIN=<nazwa użytkownika> /pKLPASSWD=<hasło> /s /x`
LUB
`msiexec.exe /x <GUID> KLLLOGIN=<nazwa użytkownika> KLPASSWD=<hasło> /qn`

Na przykład:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLLOGIN=KLAdmin  
KLPASSWD=!Password1 /qn
```

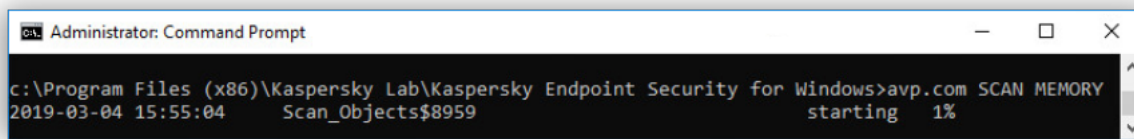
Polecenia AVP

W celu zarządzania Kaspersky Endpoint Security z poziomu wiersza poleceń:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.
3. W celu wykonania polecenia, wpisz:

```
avp.com <polecenie> [opcje]
```

W rezultacie Kaspersky Endpoint Security wykona polecenie (patrz rysunek poniżej).



Zarządzanie aplikacją z poziomu wiersza poleceń

SCAN. Skanowanie antywirusowe

Uruchamia zadanie skanowania w poszukiwaniu wirusów.

Składnia polecenia

```
SCAN [<obszar skanowania>] [<działanie po wykryciu zagrożenia>] [<typy plików>]
[<wykluczenia ze skanowania>] [/R[A]:<plik raportu>] [<technologie skanowania>] [/C:
<plik z ustawieniami skanowania>]
```

Obszar skanowania	
<pliki do skanowania>	Rozdzielona spacjami lista plików i folderów. Długie ścieżki muszą być ujęte w cudzysłów. Krótkie ścieżki (format MS-DOS) nie muszą być ujęte w cudzysłów. Na przykład: <ul style="list-style-type: none">"C:\Program Files (x86)\Example Folder" – długa ścieżka.C:\PROGRA~2\EXAMPL~1 – krótka ścieżka.
/ALL	Uruchamia zadanie <i>Pełne skanowanie</i> . Kaspersky Endpoint Security skanuje następujące obiekty: <ul style="list-style-type: none">Pamięć jądraObiekty uruchamiane wraz ze startem systemu operacyjnegoSektory startowe.Kopię zapasową systemu operacyjnegoWszystkie dyski twarde i wymienne.
/MEMORY	Skanuje pamięć jądra
/STARTUP	Skanuje obiekty uruchamiane wraz ze startem systemu operacyjnego
/MAIL	Skanuje skrzynkę pocztową programu Outlook
/REMDRIVES	Skanuje nośniki wymienne.

/FIXDRIVES	Skanuje dyski twarde.
/NETDRIVES	Skanuje dyski sieciowe.
/QUARANTINE	Skanuje pliki w Kopii zapasowej Kaspersky Endpoint Security.
/@:<file list.lst>	<p>Skanuje pliki i foldery z listy. Każdy plik na liście musi znajdować się w nowym wierszu. Długie ścieżki muszą być ujęte w cudzysłów. Krótkie ścieżki (format MS-DOS) nie muszą być ujęte w cudzysłów. Na przykład:</p> <ul style="list-style-type: none"> "C:\Program Files (x86)\Example Folder" – długa ścieżka. C:\PROGRA~2\EXAMPL~1 – krótka ścieżka.

Działanie podejmowane w przypadku wykrycia zagrożenia	
/i0	Informuj. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.
/i1	Wylecz; blokuj, jeśli leczenie nie jest możliwe. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie nie jest możliwe, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń.
/i2	<p>Wylecz; usuń, jeśli leczenie nie jest możliwe. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki.</p> <p>To ustawienie jest wybrane domyślnie.</p>
/i3	Leczy zainfekowane pliki, które zostaną wykryte. Jeśli leczenie nie powiedzie się, aplikacja usunie zainfekowane pliki. Usunie także pliki złożone (na przykład, archiwa), jeśli zainfekowanego pliku nie można wyleczyć ani usunąć.
/i4	Usuwa zainfekowane pliki. Usunie także pliki złożone (na przykład, archiwa), jeśli zainfekowanego pliku nie można usunąć.
/i8	Wyświetla pytanie o akcję, gdy tylko zostanie wykryte zagrożenie.
/i9	Po zakończeniu skanowania wyświetla pytanie o akcję.

Typy plików	
/fe	Pliki skanowane według rozszerzenia. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował tylko infekowalne pliki . Format pliku będzie określany w oparciu o jego rozszerzenie.
/fi	Pliki skanowane według formatu. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował tylko infekowalne pliki . Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików.
/fa	<p>Wszystkie pliki. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia).</p> <p>Jest to ustawienie domyślne.</p>

Wykluczenia ze skanowania	
-e:a	Archiwa RAR, ARJ, ZIP, CAB, LHA, JAR i ICE są wyłączone z obszaru skanowania.
-e:b	Bazy danych poczty, przychodzące i wychodzące wiadomości e-mail są wyłączone z obszaru skanowania.
-e:<maska pliku>	Pliki odpowiadające masce pliku są wykluczone z obszaru skanowania. Na przykład: <ul style="list-style-type: none"> Maska *.exe będzie zawierała wszystkie ścieżki do plików, które posiadają rozszerzenie exe. Maska example* będzie zawierała wszystkie ścieżki do plików o nazwie EXAMPLE.
-e:<sekundy>	Pliki, których skanowanie trwa dłużej niż określony limit czasu (w sekundach) są wykluczane z obszaru skanowania.
-es:<megabajty>	Pliki większe niż określony limit rozmiaru (w megabajtach) są wykluczane z obszaru skanowania.

Tryb zapisywania zdarzeń do pliku raportu	
/R:<plik raportu>	Zapisuje tylko krytyczne zdarzenia do pliku raportu.
/RA:<plik raportu>	Zapisuje wszystkie zdarzenia do pliku raportu.

Technologie skanowania	
/iChecker=on off	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczenie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).
/iSwift=on off	Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczenie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.

Ustawienia zaawansowane	
/C:<plik z ustawieniami skanowania antywirusowego>	Plik z ustawieniami zadania Skanowanie antywirusowe. Plik należy utworzyć ręcznie i zapisać w formacie TXT. Plik może mieć następującą zawartość: [<obszar skanowania>] [<działanie po wykryciu zagrożenia>] [<typy plików>] [<wykluczenia ze skanowania>] [/R[A]:<plik raportu>] [<technologie skanowania>].

Na przykład:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. Aktualizowanie baz danych i modułów aplikacji

Uruchamia zadanie *Aktualizacja*.

Składnia polecenia

```
UPDATE [local] ["<źródło uaktualnień>"] [/R[A]:<plik raportu>] [/C:<plik z ustawieniami aktualizacji>]
```

Ustawienia zadania aktualizacji	
local	<p>Uruchom zadanie <i>Aktualizacja</i>, które zostało utworzone automatycznie po zainstalowaniu aplikacji. Możesz zmienić ustawienia zadania <i>Aktualizacja</i> w lokalnym interfejsie aplikacji lub w konsoli Kaspersky Security Center. Jeśli to ustawienie nie zostało skonfigurowane, Kaspersky Endpoint Security uruchamia zadanie <i>Aktualizacja</i> z domyślnymi ustawieniami lub z ustawieniami określonymi w poleceniu. Możesz skonfigurować ustawienia zadania <i>Aktualizacja</i> w następujący sposób:</p> <ul style="list-style-type: none">• UPDATE uruchamia zadanie <i>Aktualizacja</i> z ustawieniami domyślnymi: źródło uaktualnień to serwery aktualizacji Kaspersky, konto to System i inne ustawienia domyślne.• UPDATE local uruchamia zadanie <i>Aktualizacja</i>, które zostało utworzone automatycznie po instalacji (predefiniowane zadanie).• UPDATE <ustawienia aktualizacji> uruchamia zadanie <i>Aktualizacja</i> z ręcznie zdefiniowanymi ustawieniami (patrz poniżej).

Źródło aktualizacji	
"<źródło uaktualnień>"	<p>Adres serwera HTTP lub FTP lub folderu współdzielonego z pakietem aktualizacji. Możesz określić tylko jedno źródło uaktualnień. Jeśli źródło uaktualnień nie zostało określone, Kaspersky Endpoint Security korzysta z domyślnego źródła: serwery aktualizacji Kaspersky.</p>

Tryb zapisywania zdarzeń do pliku raportu	
/R:<plik raportu>	Zapisuje tylko krytyczne zdarzenia do pliku raportu.
/RA:<plik raportu>	Zapisuje wszystkie zdarzenia do pliku raportu.

Ustawienia zaawansowane	
/C: <plik z ustawieniami aktualizacji>	<p>Plik z ustawieniami zadania <i>Aktualizacja</i>. Plik należy utworzyć ręcznie i zapisać w formacie TXT. Plik może mieć następującą zawartość: ["<źródło uaktualnień>"] [/R[A]:<plik raportu>].</p>

Na przykład:

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. Wycofanie ostatniej aktualizacji

Wycofuje ostatnią aktualizację antywirusowych baz danych. Umożliwi to w razie czego wycofanie baz danych i modułów aplikacji do ich poprzedniej wersji, na przykład, gdy nowa wersja baz danych zawiera nieprawidłową sygnaturę powodującą, że Kaspersky Endpoint Security blokuje bezpieczną aplikację.

Składnia polecenia

```
ROLLBACK [/R[A]:<plik raportu>]
```

Tryb zapisywania zdarzeń do pliku raportu	
/R:<plik raportu>	Zapisuje tylko krytyczne zdarzenia do pliku raportu.
/RA:<plik raportu>	Zapisuje wszystkie zdarzenia do pliku raportu.

Na przykład:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. Śledzenie

Włącza/wyłącza śledzenie. [Pliki śledzenia](#) są przechowywane na komputerze tak długo, jak aplikacja jest używana i są trwale usuwane, gdy aplikacja jest usuwana. Pliki śledzenia, za wyjątkiem plików śledzenia Agenta autoryzacji, są przechowywane w folderze %ProgramData%\Kaspersky Lab\KES\Traces. Domyślnie śledzenie jest wyłączone.

Składnia polecenia

```
TRACES on|off [<poziom śledzenia>] [<ustawienia zaawansowane>]
```

Poziom śledzenia	
<poziom śledzenia>	<p>Poziom szczegółowości śledzenia. Dostępne wartości:</p> <ul style="list-style-type: none">• 100 (krytyczny). Tylko wiadomości dotyczące błędów krytycznych.• 200 (wysoki). Wiadomości o wszystkich błędach, w tym błędach krytycznych.• 300 (diagnostyczny). Wiadomości o wszystkich błędach, a także ostrzeżenia.• 400 (ważny). Wszystkie wiadomości o błędach, ostrzeżenia i dodatkowe informacje.• 500 (normalny). Wiadomości o wszystkich błędach i ostrzeżeniach, a także szczegółowe informacje o działaniu aplikacji w trybie normalnym (domyślnie).• 600 (niski). Wszystkie wiadomości.

Ustawienia zaawansowane	
all	Uruchamia polecenie z parametrami <code>dbg</code> , <code>file</code> i <code>mem</code> .
dbg	Włącza funkcję <code>OutputDebugString</code> i zapisuje plik śledzenia. Funkcja <code>OutputDebugString</code> wysyła ciąg znaków do debugera aplikacji w celu wyświetlenia na ekranie. Aby uzyskać szczegółowe informacje, odwiedź stronę internetową MSDN .
file	Zapisuje jeden plik śledzenia (bez ograniczenia rozmiaru).
rot	Zapisuje ślady do ograniczonej liczby plików o ograniczonym rozmiarze i nadpisuje starsze pliki po osiągnięciu maksymalnego rozmiaru.
mem	Zapisuje ślady do plików zrzutów.

Na przykład:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES on 500 dbg mem`
- `avp.com TRACES off file`

START. Uruchamianie profilu

Uruchamia profil (na przykład, aby zaktualizować bazy danych lub włączyć składnik ochrony).

Składnia polecenia

```
START <profil> [/R[A]:<plik raportu>]
```

Profil	
<profil>	Nazwa profilu. <i>Profil</i> to komponent, zadanie lub funkcja Kaspersky Endpoint Security. Możesz wyświetlić listę dostępnych profilu , wykonując polecenie <code>HELP START</code> .

Tryb zapisywania zdarzeń do pliku raportu	
<code>/R:<plik raportu></code>	Zapisuje tylko krytyczne zdarzenia do pliku raportu.
<code>/RA:<plik raportu></code>	Zapisuje wszystkie zdarzenia do pliku raportu.

Na przykład:

```
avp.com START Scan_Objects
```

STOP. Zatrzymywanie profilu

Zatrzymuje uruchomiony profil (na przykład, zatrzymuje skanowanie, zatrzymuje skanowanie dysków wymiennych lub wyłącza składnik ochrony).

Aby wykonać to polecenie, [Ochrona hasłem musi być włączona](#). Użytkownik musi mieć uprawnienia **Wyłączenie składników ochrony** i **Wyłączenie składników kontroli**.

Składnia polecenia

```
STOP <profil> /login=<nazwa użytkownika> /password=<hasło>
```

Profil	
<profil>	Nazwa profilu. <i>Profil</i> to komponent, zadanie lub funkcja Kaspersky Endpoint Security. Możesz wyświetlić listę dostępnych profilu , wykonując polecenie <code>HELP STOP</code> .

Autoryzacja	
<code>/login=<nazwa użytkownika></code> <code>/password=<hasło></code>	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem .

STATUS. Stan profilu

Wyświetla informacje o stanie dla [profilu aplikacji](#) (na przykład: `uruchomione` lub `zakończone`). Listę dostępnych profili można wyświetlić, wykonując polecenie `HELP STATUS`.

Kaspersky Endpoint Security wyświetla również informacje o stanie profili usług. Informacje o stanie profili usług mogą być wymagane podczas kontaktu z pomocą techniczną Kaspersky.

Składnia polecenia

```
STATUS [<profil>]
```

STATISTICS. Statystyki działania profilu

Wyświetlanie informacji statystycznych dotyczących [profilu aplikacji](#) (na przykład, czasu trwania skanowania lub liczby wykrytych zagrożeń). Listę dostępnych profili można wyświetlić, wykonując polecenie `HELP STATISTICS`.

Składnia polecenia

```
STATISTICS <profil>
```


RESTORE. Przywracanie plików z Kopii zapasowej

Możliwe jest przywrócenie pliku z Kopii zapasowej do jego oryginalnego folderu. Jeżeli plik o tej samej nazwie istnieje już w podanej ścieżce, do nazwy pliku dołączany jest przyrostek „-copy”. Przywracany plik jest kopiowany z zachowaniem oryginalnej nazwy.

Aby wykonać to polecenie, [Ochrona hasłem musi być włączona](#). Użytkownik musi posiadać uprawnienie **Przywróć z Kopii zapasowej**.

Kopia zapasowa przechowuje zapasowe kopie plików, które zostały usunięte lub zmodyfikowane podczas leczenia. *Kopia zapasowa* to kopia pliku utworzona przed wyleczeniem lub usunięciem pliku. Kopie zapasowe plików są przechowywane w specjalnym formacie i nie stanowią zagrożenia.

Kopie zapasowe plików są przechowywane w folderze C:\ProgramData\Kaspersky Lab\KES\QB.

Użytkownicy należący do grupy Administratorzy mają nadane pełne uprawnienie dostępu do tego folderu. Ograniczone uprawnienia dostępu do tego folderu są nadawane użytkownikom, których konto zostało użyte do zainstalowania Kaspersky Endpoint Security.

Kaspersky Endpoint Security nie oferuje możliwości skonfigurowania uprawnień dostępu użytkownika do kopii zapasowych plików.

Składnia polecenia

```
RESTORE [/REPLACE] <nazwa pliku> /login=<nazwa użytkownika> /password=<hasło>
```

Ustawienia zaawansowane	
/REPLACE	Nadpisuje istniejący plik.
<nazwa pliku>	Nazwa pliku, który ma zostać przywrócony.

Autoryzacja	
/login=<nazwa użytkownika> /password=<hasło>	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem .

Na przykład:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. Eksportowanie ustawień aplikacji

Eksportuje ustawienia Kaspersky Endpoint Security do pliku. Plik będzie znajdował się w folderze C:\Windows\SysWOW64.

Składnia polecenia

```
EXPORT <profil> <nazwa pliku>
```

Profil	
<profil>	Nazwa profilu. <i>Profil</i> to komponent, zadanie lub funkcja Kaspersky Endpoint Security. Listę dostępnych profilu można wyświetlić, wykonując polecenie <code>HELP EXPORT</code> .

Plik do wyeksportowania	
<nazwa pliku>	Nazwa pliku, do którego będą eksportowane ustawienia aplikacji. Ustawienia Kaspersky Endpoint Security można wyeksportować do pliku konfiguracyjnego DAT lub CFG, pliku tekstowego TXT lub dokumentu XML.

Na przykład:

- `avp.com EXPORT ids ids_config.dat`
- `avp.com EXPORT fm fm_config.txt`

IMPORT. Importowanie ustawień aplikacji

Importuje ustawienia dla Kaspersky Endpoint Security z pliku utworzonego za pomocą polecenia `EXPORT`.

Aby wykonać to polecenie, [Ochrona hasłem musi być włączona](#). Użytkownik musi posiadać uprawnienie **Konfiguracja ustawień aplikacji**.

Składnia polecenia

```
IMPORT <nazwa pliku> /login=<nazwa użytkownika> /password=<hasło>
```

Plik do importu	
<nazwa pliku>	Nazwa pliku, z którego będą importowane ustawienia aplikacji. Ustawienia Kaspersky Endpoint Security można zaimportować z pliku konfiguracyjnego DAT lub CFG, pliku tekstowego TXT lub dokumentu XML.

Autoryzacja	
<code>/login=<nazwa użytkownika></code> <code>/password=<hasło></code>	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem .

Na przykład:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. Zastosowanie pliku klucza

Stosuje plik klucza, aby aktywować Kaspersky Endpoint Security. Jeśli aplikacja została już aktywowana, klucz zostanie dodany jako zapasowy.

Składnia polecenia

```
ADDKEY <nazwa pliku> /login=<nazwa użytkownika> /password=<hasło>
```

Plik klucza	
<nazwa pliku>	Nazwa pliku klucza.

Autoryzacja	
/login=<nazwa użytkownika> /password=<hasło>	Dane uwierzytelniające konto użytkownika. Dane te należy wprowadzić tylko wtedy, gdy włączona jest Ochrona hasłem .

Na przykład:

```
avp.com ADDKEY file.key
```

LICENSE. Licencjonowanie

Wykonuje czynności związane z kluczami licencyjnymi Kaspersky Endpoint Security.

Aby wykonać to polecenie i usunąć klucz licencyjny, [Ochrona hasłem musi być włączona](#). Użytkownik musi posiadać uprawnienie **Usuwanie klucza**.

Składnia polecenia

```
LICENSE <działanie> [/login=<nazwa użytkownika> /password=<hasło>]
```

Działanie	
/ADD <nazwa pliku>	Stosuje plik klucza, aby aktywować Kaspersky Endpoint Security. Jeśli aplikacja została już aktywowana, klucz zostanie dodany jako zapasowy.
/ADD <kod aktywacyjny>	Aktywuje Kaspersky Endpoint Security przy użyciu kodu aktywacyjnego. Jeśli aplikacja została już aktywowana, klucz zostanie dodany jako zapasowy.
/REFRESH <nazwa pliku>	Odnawia licencję za pomocą pliku klucza. W rezultacie zostanie dodany klucz zapasowy. Stanie się aktywny po wygaśnięciu licencji. Nie jest możliwe dodanie aktywnego klucza przez wykonanie tego polecenia.
/REFRESH <kod aktywacyjny>	Odnawia licencję za pomocą kodu aktywacyjnego. W rezultacie zostanie dodany klucz zapasowy. Stanie się aktywny po wygaśnięciu licencji. Nie jest możliwe dodanie aktywnego klucza przez wykonanie tego polecenia.
/DEL /login=	Usuwa klucz licencyjny. Klucz zapasowy również zostanie usunięty.

```
<nazwa
użytkownika>
/password=<hasło>
```

Autoryzacja

```
/login=<nazwa użytkownika>
/password=<hasło>
```

Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami [Ochrony hasłem](#).

Na przykład:

- avp.com LICENSE /ADD file.key
- avp.com LICENSE /ADD AAAAAA-BBBBBB-CCCCCC-DDDDDD
- avp.com LICENSE /DEL /login=KLAdmin /password=!Password1

RENEW. Kupowanie licencji

Otwiera stronę internetową Kaspersky, na której można kupić lub odnowić licencję.

PBATESTRESET. Resetowanie wyników sprawdzania dysku przed zaszyfrowaniem dysku

Zresetuj wyniki sprawdzania kompatybilności Szyfrowania całego dysku (FDE), w tym obu technologii Kaspersky Disk Encryption i Szyfrowanie dysków funkcją BitLocker.

Przed uruchomieniem Szyfrowania całego dysku aplikacja przeprowadza szereg kontroli w celu sprawdzenia, czy komputer może zostać zaszyfrowany. Jeśli komputer nie obsługuje Szyfrowania całego dysku, Kaspersky Endpoint Security rejestruje informacje o braku kompatybilności. Następnym razem, gdy spróbujesz zaszyfrować komputer, aplikacja nie wykona tego sprawdzenia i wyświetli ostrzeżenie informujące, że szyfrowanie nie jest możliwe. Jeśli konfiguracja sprzętowa komputera uległa zmianie, wyniki kontroli kompatybilności wcześniej zarejestrowane przez aplikację należy zresetować, aby ponownie sprawdzić systemowy dysk twardy pod kątem zgodności z technologiami Kaspersky Disk Encryption i Szyfrowanie dysków funkcją BitLocker.

EXIT. Zakończenie działania aplikacji

Kończy działanie Kaspersky Endpoint Security. Aplikacja zostanie wyładowana z pamięci RAM komputera.

Aby wykonać to polecenie, [Ochrona hasłem musi być włączona](#). Użytkownik musi posiadać uprawnienie **Zakończenie działania aplikacji**.

Składnia polecenia

```
EXIT /login=<nazwa użytkownika> /password=<hasło>
```

EXITPOLICY. Wyłączanie profilu

Wyłącza profil Kaspersky Security Center na komputerze. Wszystkie ustawienia Kaspersky Endpoint Security są dostępne do konfiguracji, włącznie z ustawieniami, które mają zamkniętą kłódkę w profilu (🔒).

Aby wykonać to polecenie, [Ochrona hasłem musi być włączona](#). Użytkownik musi mieć uprawnienie **Wyłączenie zasady Kaspersky Security Center**.

Składnia polecenia

```
EXITPOLICY /login=<nazwa użytkownika> /password=<hasło>
```

STARTPOLICY. Włączanie profilu

Włącza profil Kaspersky Security Center na komputerze. Ustawienia aplikacji zostaną skonfigurowane zgodnie z profilem.

DISABLE. Wyłączanie ochrony

Wyłącza Ochronę plików na komputerze z licencją dla Kaspersky Endpoint Security, która utraciła ważność. Nie można uruchomić tego polecenia na komputerze, na którym aplikacja nie została aktywowana lub posiada ważną licencję.

SPYWARE. Wykrywanie oprogramowania szpiegującego

Włącz/wyłącz wykrywanie programów szpiegujących. Domyślnie wykrywanie programów szpiegujących jest włączone.

Składnia polecenia

```
SPYWARE on|off
```

KSN. Przeniesienie Globalnej / Prywatnej sieci KSN

Wybieranie rozwiązania Kaspersky Security Network do określania reputacji plików lub stron internetowych. Kaspersky Endpoint Security obsługuje następujące rozwiązania infrastrukturalne KSN:

- *Globalna sieć KSN* to rozwiązanie używane przez większość aplikacji Kaspersky. Uczestnicy KSN otrzymują informacje z Kaspersky Security Network i wysyłają do Kaspersky informacje o obiektach wykrytych na komputerze użytkownika w celu dodatkowego przeanalizowania przez analityków Kaspersky i znajdujących się w bazach danych reputacji oraz statystycznych bazach danych usługi Kaspersky Security Network.

- *Prywatna sieć KSN* to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów. Prywatna sieć KSN została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z dowolnego z następujących powodów:
 - Lokalne stacje robocze nie są połączone z internetem.
 - Przesyłanie wszelkich danych poza kraj lub poza korporacyjną sieć LAN są zabronione przez prawo lub ograniczone przez politykę bezpieczeństwa firmy.

Składnia polecenia

```
KSN /global | /private <nazwa pliku>
```

Plik konfiguracyjny Prywatnej sieci KSN	
<nazwa pliku>	Nazwa pliku konfiguracyjnego zawierającego ustawienia serwera proxy KSN Ten plik posiada rozszerzenie PKCS7 lub PEM.

Na przykład:

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

Polecenia KESCLI

Polecenia KESCLI umożliwiają odbieranie informacji o stanie ochrony komputera przy użyciu komponentu OPSWAT oraz umożliwiają wykonanie standardowych zadań, takich jak skanowania antywirusowe i aktualizacje baz danych.

Możesz przejrzeć listę poleceń KESCLI, korzystając z polecenia `--help` lub używając skróconego polecenia `-h`.

W celu zarządzania Kaspersky Endpoint Security z poziomu wiersza poleceń:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu, w którym znajduje się plik wykonywalny Kaspersky Endpoint Security.
3. W celu wykonania polecenia, wpisz:

```
kescli <polecenie> [opcje]
```

W rezultacie Kaspersky Endpoint Security wykona polecenie (patrz rysunek poniżej).

```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File"      1      3/16/2021 17:14:37      "https://secure.eicar.org/eicar.com.txt"      41      1
"EICAR-Test-File"      1      3/16/2021 17:14:38      "https://www.eicar.org/download/eicar.com"     41      1
```

Zarządzanie aplikacją z poziomu wiersza poleceń

Skanowanie. Skanowanie antywirusowe

Uruchamia zadanie skanowania w poszukiwaniu wirusów.

Składnia polecenia

```
--opswat Scan <obszar skanowania> <działanie podejmowane w przypadku wykrycia zagrożenia>
```

Możesz sprawdzić stan zakończenia zadania *Pełne skanowanie*, korzystając z polecenia [GetScanState](#) i sprawdzając datę i godzinę zakończenia ostatniego skanowania przy użyciu polecenia [GetLastScanTime](#).

Obszar skanowania	
<pliki do skanowania>	; -rozdzielona spacjami lista plików i folderów. Na przykład: C:\Program Files (x86)\Example Folder.

Działanie podejmowane w przypadku wykrycia zagrożenia	
0	Informuj. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security doda informacje o zainfekowanych plikach do listy aktywnych zagrożeń po wykryciu tych plików.
1	Wylecz; usuń, jeśli leczenie nie jest możliwe. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki. To ustawienie jest wybrane domyślnie.

Na przykład:

```
kescli --opswat Scan C:\Documents and Settings\All Users\My Documents;C:\Program Files 1
```

GetScanState. Stan zakończenia skanowania

Uzyskaj informacje o stanie zakończenia zadania *Pełne skanowanie*:

- 1 – skanowanie jest wykonywane.

- 0 – skanowanie nie zostało uruchomione.

Składnia polecenia

```
--opswat GetScanState
```

Na przykład:

```
kescli --opswat GetScanState
```

GetLastScanTime. Określanie czasu zakończenia skanowania

Uzyskaj informacje o dacie i godzinie zakończenia ostatniego zadania *Pełne skanowanie*.

Składnia polecenia

```
--opswat GetLastScanTime
```

Na przykład:

```
kescli --opswat GetLastScanTime
```

GetThreats. Uzyskiwanie danych dotyczących wykrytych zagrożeń

Uzyskaj listę wykrytych zagrożeń (*Raport dotyczący zagrożeń*). Ten raport zawiera informacje o zagrożeniach i aktywności wirusów w ciągu ostatnich 30 dni przed utworzeniem raportu.

Składnia polecenia

```
--opswat GetThreats
```

Po wykonaniu tego polecenia, Kaspersky Endpoint Security wyśle odpowiedź w następującym formacie:

```
<nazwa wykrytego obiektu> <typ obiektu> <data i wykrycia obiektu> <ścieżka do pliku>  
<działanie podejmowane w przypadku wykrycia zagrożenia> <poziom zagrożenia>
```

```
Administrator: Command Prompt
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security for Windows>kescli --opswat GetThreats
"EICAR-Test-File" 1 3/16/2021 17:14:37 "https://secure.eicar.org/eicar.com.txt" 41 1
"EICAR-Test-File" 1 3/16/2021 17:14:38 "https://www.eicar.org/download/eicar.com" 41 1
```

Zarządzanie aplikacją z poziomu wiersza poleceń

Typ obiektu	
0	Nieznany (Nieznany).
1	Wirusy (Virware).

2	Programy typu trojan (Trojware).
3	Szkodliwe programy (Szkodliwe oprogramowanie).
4	Programy reklamowe (Adware).
5	Auto-dialery (Pornware).
6	Aplikacje, które mogły zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych użytkownika (Riskware).
7	Obiekty spakowane, których metoda pakowania może być używana do ochrony szkodliwego kodu (Spakowane).
20	Nieznane obiekty (Xfiles).
21	Znane aplikacje (Oprogramowanie).
22	Ukryte pliki (Ukryte).
23	Aplikacja wymagająca uwagi (Pupware).
24	Nietypowe zachowanie (Anomalia).
30	Niezdefiniowany (Niewykryty).
40	Banery reklamowe (Baner).
50	Atak sieciowy (Atak).
51	Dostęp do rejestru (Rejestr).
52	Podważana aktywność (Podważenie).
60	Luki (Luka).
70	Phishing.
80	Niechciany załącznik poczty e-mail (Załącznik).
90	Szkodliwe oprogramowanie wykryte przez Kaspersky Security Network (Pilne).
100	Nieznany odnośnik (Podważany URL).
110	Inne szkodliwe oprogramowanie (Behawioralny).

Działanie podejmowane w przypadku wykrycia zagrożenia	
0	Nieznany (nieznany).
1	Zagrożenie zostało skorygowane (ok).
2	Obiekt został zainfekowany i nie został wyleczony (zainfekowany).
5	Obiekt jest w archiwum i nie został wyleczony (archiwum).
9	Obiekt został wyleczony (wyleczony).
10	Obiekt nie został wyleczony (niewyleczony).
11	Obiekt został usunięty (usunięto).
13	Utworzono kopię zapasową obiektu (utworzono kopię zapasową).
15	Obiekt został przeniesiony do Kopii zapasowej (poddany kwarantannie).
23	Obiekt został usunięty po ponownym uruchomieniu komputera (usunięty)

	po ponownym uruchomieniu).
25	Obiekt został wyleczony po ponownym uruchomieniu komputera (wylecz po ponownym uruchomieniu).
29	Obiekt został przeniesiony do Kopii zapasowej przez użytkownika (dodany przez użytkownika).
30	Obiekt został dodany do wykluczeń (dodany do wykluczeń).
31	Obiekt został przeniesiony do Kopii zapasowej po ponownym uruchomieniu komputera (poddany kwarantannie po ponownym uruchomieniu komputera).
36	Fałszywy alarm (fałszywy alarm).
38	Proces został przerwany (przerwany).
40	Obiekt nie został wykryty (nie odnaleziono).
41	Nie można rozpoznać zagrożenia (nie można wyleczyć).
42	Obiekt został przywrócony (wycofano).
43	Obiekt został utworzony w wyniku aktywności zagrożenia (utworzony przez zagrożenie).
44	Obiekt został przywrócony po ponownym uruchomieniu komputera (wycofany po ponownym uruchomieniu).
0xffffffff	Obiekt nie został przetworzony (odrzucono).

Poziom zagrożenia	
0	Nieznany
1	Wysoki
2	Średni
4	Niski
8	Informacja (mniej niż <i>Niski</i>)

UpdateDefinitions. Aktualizowanie baz danych i modułów aplikacji

Uruchamia zadanie *Aktualizacja*. Kaspersky Endpoint Security korzysta z domyślnego źródła: serwery aktualizacji Kaspersky.

Składnia polecenia

```
--opswat UpdateDefinitions
```

Możesz przejrzeć datę i godzinę ostatniego zakońzonego zadania *Aktualizacja*, korzystając z polecenia [GetDefinitionsetState](#).

Na przykład:

```
kescli --opswat UpdateDefinitions
```

GetDefinitionState. Określanie czasu zakończenia aktualizacji

Uzyskaj informacje o dacie i godzinie zakończenia ostatniego zadania *Aktualizacja*.

Składnia polecenia

```
--opswat GetDefinitionState
```

Na przykład:

```
kescli --opswat GetDefinitionState
```

EnableRTP. Włączanie ochrony

Włącz składniki ochrony Kaspersky Endpoint Security na komputerze: Ochrona plików, Ochrona WWW, Ochrona poczty, Ochrona sieci, Ochrona przed włamaniami.

Składnia polecenia

```
--opswat EnableRTP
```

Możesz sprawdzić stan działania Ochrony plików, korzystając z polecenia [GetRealTimeProtectionState](#).

Na przykład:

```
kescli --opswat EnableRTP
```

GetRealTimeProtectionState. Stan Ochrony plików

Uzyskaj informacje o stanie działania komponentu Ochrona plików:

- 1 – komponent jest włączony.
- 0 – komponent jest wyłączony.

Składnia polecenia

```
--opswat GetRealTimeProtectionState
```

Na przykład:

```
kescli --opswat GetRealTimeProtectionState
```

Wersja. Identyfikowanie wersji aplikacji

Zidentyfikuj wersję Kaspersky Endpoint Security for Windows.

Składnia polecenia

```
--Version
```

Możesz także użyć skróconego polecenia `-v`.

Na przykład:
`kescli -v`

Polecenia zarządzania Detection and Response

Możesz użyć wiersza polecenia do zarządzania wbudowaną funkcjonalnością rozwiązań Detection and Response (na przykład, Kaspersky Sandbox lub Kaspersky Endpoint Detection and Response Optimum). Możesz zarządzać rozwiązaniami Detection and Response, jeśli zarządzanie przy użyciu konsoli Kaspersky Security Center nie jest możliwe. Możesz wyświetlić listę poleceń do zarządzania aplikacją, wykonując polecenie `HELP`. Aby zapoznać się z informacjami o składni konkretnego polecenia, wpisz `HELP <polecenie>`.

SANDBOX. Zarządzanie Kaspersky Sandbox

Polecenia do zarządzania komponentem Kaspersky Sandbox:

- Włącz lub wyłącz komponent Kaspersky Sandbox.
Komponent Kaspersky Sandbox włącza współdziałanie z rozwiązaniem Kaspersky Sandbox.
- Skonfiguruj komponent Kaspersky Sandbox:
 - Podłącz komputer do serwerów Kaspersky Sandbox.
Serwery używają wdrożonych obrazów wirtualnych systemów operacyjnych Microsoft Windows do uruchamiania obiektów, które muszą zostać przeskanowane. Możesz wprowadzić adres IP (IPv4 lub IPv6) lub w pełni kwalifikowaną nazwę domeny. Więcej informacji dotyczących wdrożenia obrazów wirtualnych i skonfigurowania serwerów Kaspersky Sandbox można znaleźć w *pomocy dla [Kaspersky Sandbox](#)*.
 - Skonfiguruj limit czasu połączenia dla serwera Kaspersky Sandbox.
Przekroczenie limitu czasu dla otrzymania odpowiedzi na żądanie skanowania obiektu z serwera Kaspersky Sandbox. Po upływie czasu, Kaspersky Sandbox przekieruje żądanie do następnego serwera. Wartość przekroczenia limitu czasu zależy od prędkości i stabilności połączenia. Domyślnie wynosi on 5 sekund.
 - Skonfiguruj zaufane połączenie między komputerem a serwerami Kaspersky Sandbox.
Aby skonfigurować zaufane połączenie z serwerami Kaspersky Sandbox, musisz przygotować certyfikat TLS. Następnie musisz dodać certyfikat do serwerów Kaspersky Sandbox i zasady Kaspersky Endpoint Security. Więcej informacji na temat przygotowywania certyfikatu i dodawania certyfikatu do serwerów znajdziesz w *pomocy dla Kaspersky Sandbox*.
- Wyświetla bieżące ustawienia komponentu.

Składnia polecenia

```
stop sandbox [/login=<nazwa użytkownika> /password=<hasło>]
start sandbox
sandbox /set [--tls=yes|no] [--servers=<adres serwera>:<port>] [--timeout=<limit
czasu połączenia z serwerem Kaspersky Sandbox został przekroczony (ms)>] [--pinned-
certificate=<ścieżka do certyfikatu TLS>][/login=<nazwa użytkownika> /password=
<hasło>]
sandbox /show
```

Działanie	
stop	Wyłącza komponent Kaspersky Sandbox.
start	Włącza komponent Kaspersky Sandbox.
set	Konfiguruje komponent Kaspersky Sandbox. Możesz zmodyfikować następujące ustawienia: <ul style="list-style-type: none"> • Użyj zaufanego połączenia (--tls). • Dodaj certyfikat TLS (--pinned-certificate). • Skonfiguruj limit czasu połączenia z serwerem Kaspersky Sandbox (--timeout). • Dodaje serwery Kaspersky Sandbox (--servers).
show	Wyświetla bieżące ustawienia komponentu. Otrzymasz następującą odpowiedź: <pre>sandbox.timeout=<limit czasu połączenia z serwerem Kaspersky Sandbox został przekroczony (ms)> sandbox.tls=<stan zaufanego połączenia> sandbox.servers=<lista serwerów Kaspersky Sandbox></pre>

Autoryzacja	
/login=<nazwa użytkownika> /password=<hasło>	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem .

Na przykład:

```
avp.com start sandbox
avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem"
avp.com sandbox /set --servers=10.10.111.0:147
```

PREVENTION. Zarządzanie zapobieganiem wykonaniu

Wyłącz Zapobieganie wykonywaniu lub wyświetl bieżące ustawienia komponentu, w tym listę reguł zapobiegania wykonywaniu.

Składnia polecenia

```
prevention disable
prevention /show
```

Po wykonaniu polecenia `prevention /show` uzyskasz następującą odpowiedź:

prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <identyfikator reguły>

target: script|process|document

md5: <suma kontrolna MD5 pliku>

sha256: <suma kontrolna SHA256 pliku>

pattern: <ścieżka do obiektu>

case-sensitive: true|false

Wartości zwrotne polecenia:

- -1 oznacza, że polecenie nie jest obsługiwane przez wersję Kaspersky Endpoint Agent, który jest zainstalowany na urządzeniu.
- 0 oznacza, że polecenie zostało wykonane pomyślnie.
- 1 oznacza, że obowiązkowy argument nie został przekazany do polecenia.
- 2 oznacza, że wystąpił ogólny błąd.
- 4 oznacza, że wystąpił błąd składniowy.
- 9 – błędna operacja (na przykład, próba wyłączenia komponentu, gdy jest już wyłączony).

ISOLATION. Zarządzanie Izolacją sieci

Wyłącz Izolację sieci dla komputera lub wyświetl bieżące ustawienia komponentu, w tym listę skonfigurowanych profili wykluczeń sieci, a także listę reguł skonfigurowanych w profilach sieci.

Składnia polecenia:

```
isolation /OFF /login=<nazwa użytkownika> /password=<hasło>  
isolation /STAT
```

W wyniku uruchomienia polecenia `show` otrzymujesz następującą odpowiedź: `isolation.enable=true|false`.

Wartości zwrotne polecenia:

- -1 oznacza, że polecenie nie jest obsługiwane przez wersję Kaspersky Endpoint Agent, który jest zainstalowany na urządzeniu.
- 0 oznacza, że polecenie zostało wykonane pomyślnie.
- 1 oznacza, że obowiązkowy argument nie został przekazany do polecenia.
- 2 oznacza, że wystąpił ogólny błąd.

- 4 oznacza, że wystąpił błąd składniowy.
- 9 – błędna operacja (na przykład, próba wyłączenia komponentu, gdy jest już wyłączony).

RESTORE. Przywracanie plików z Kwarantanny

Przywróć plik z Kwarantanny do specjalnego folderu na komputerze. Następnie ręcznie przenieś plik do folderu docelowego. *Kwarantanna* to specjalny lokalny magazyn na komputerze, na którym zainfekowane pliki lub pliki nie dające się wyleczyć zostają przeniesione do tego właśnie katalogu. Pliki poddane kwarantannie są przechowywane w postaci zaszyfrowanej i nie zagrażają bezpieczeństwu urządzenia. Kaspersky Endpoint Security używa Kwarantanny tylko podczas pracy z rozwiązaniami Kaspersky Sandbox i Kaspersky Endpoint Detection and Response Optimum. W innych przypadkach Kaspersky Endpoint Security umieszcza odpowiedni plik w Kopii zapasowej. Więcej informacji na temat zarządzania Kwarantanną jako częścią rozwiązań można znaleźć w *podręcznikach dotyczących [Kaspersky Sandbox](#) i [Kaspersky Endpoint Detection and Response Optimum](#)*.

Aby wykonać to polecenie, [Ochrona hasłem musi być włączona](#). Użytkownik musi posiadać uprawnienie **Przywróć z Kopii zapasowej**.

Obiekt jest poddawany kwarantannie z poziomu konta systemowego (SYSTEM).

Składnia polecenia

```
RESTORE [/REPLACE] <nazwa pliku> /login=<nazwa użytkownika> /password=<hasło>
```

Ustawienia zaawansowane	
/REPLACE	Nadpisuje istniejący plik.
<nazwa pliku>	Nazwa pliku, który ma zostać przywrócony.

Autoryzacja	
/login=<nazwa użytkownika> /password=<hasło>	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem .

Na przykład:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

Wartości zwrotne polecenia:

- -1 oznacza, że polecenie nie jest obsługiwane przez wersję Kaspersky Endpoint Agent, który jest zainstalowany na urządzeniu.
- 0 oznacza, że polecenie zostało wykonane pomyślnie.
- 1 oznacza, że obowiązkowy argument nie został przekazany do polecenia.
- 2 oznacza, że wystąpił ogólny błąd.
- 4 oznacza, że wystąpił błąd składniowy.

IOCSCAN. Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (IOC)

Uruchom zadanie Skanowanie pod kątem wskaźników naruszeń bezpieczeństwa (IOC). *Wskaźnik naruszeń bezpieczeństwa (IOC)* to zestaw danych dotyczących obiektu lub aktywności, która wskazuje nieautoryzowany dostęp do komputera (naruszenie bezpieczeństwa danych). Na przykład, wiele niepomyślnych prób zalogowania do systemu może stanowić wskaźnik naruszeń bezpieczeństwa. Zadania *Skanowanie IOC* umożliwiają odszukanie wskaźników naruszeń bezpieczeństwa na komputerze i podejmują środki reakcji na zagrożenia.

Składnia polecenia

```
IOCSCAN <pełna ścieżka do pliku IOC>[/path=<ścieżka do folderu plików IOC>
[/process=on|off] [/hint=<pełna ścieżka do pliku wykonywalnego procesu|pełna ścieżka
do pliku>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off] [/ports=on|off]
[/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off]
[/eventlog=on|off] [/datetime=<data publikacji zdarzenia>] [/channels=<lista kanałów>]
[/files=on|off] [/drives=<all|system|critical|custom>] [/excludes=<lista wykluczeń>]
[/scope=<lista folderów do przeskanowania>]
```

Pliki IOC	
<pełna ścieżka do pliku IOC>	Pełna ścieżka do pliku IOC, którego chcesz użyć do skanowania. Możesz określić kilka plików IOC oddzielonych spacjami. Pełna ścieżka do pliku IOC musi zostać wprowadzona bez argumentu /path. Na przykład: C:\Users\Admin\Desktop\IOC\file1.ioc
/path=<ścieżka do folderu z plikami IOC>	Ścieżka do folderu z plikami IOC, których chcesz użyć do skanowania. <i>Pliki IOC</i> to pliki zawierające zestawy wskaźników, które aplikacja próbuje dopasować do licznika wykrywania. Pliki IOC muszą pasować do standardu OpenIOC . Na przykład: C:\Users\Admin\Desktop\IOC

Typ danych skanowania IOC	
/process=on off	Analizuje dane procesu podczas wykonywania skanowania IOC (warunek ProcessItem). Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie analizuje procesów uruchamianych na komputerze podczas wykonywania skanowania. Jeśli plik IOC zawiera warunki IOC dokumentu ProcessItem IOC, są one ignorowane (wykryte jako brak dopasowania). Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane procesu tylko wtedy, gdy dokument ProcessItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.
/hint=<pełna ścieżka dostępu do pliku wykonywalnego procesu pełna ścieżka do pliku>	Analizuje dane pliku podczas wykonywania skanowania IOC (warunki ProcessItem i FileItem). Możesz wybrać plik na jeden z następujących sposobów: <ul style="list-style-type: none"> <pełna ścieżka do pliku wykonywalnego procesu> – ProcessItem; <pełna ścieżka do pliku> – FileItem.

<p>/registry=on off</p>	<p>Analizuje dane rejestru systemu Windows podczas wykonywania skanowania IOC (warunek RegistryItem).</p> <p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie skanuje rejestru systemu Windows. Jeśli plik IOC zawiera warunki dokumentu RegistryItem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje rejestr systemu Windows tylko wtedy, gdy dokument RegistryItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p> <p>Dla typów danych RegistryItem Kaspersky Endpoint Security skanuje zestaw kluczy rejestru.</p>
<p>/dnsentry=on off</p>	<p>Analizuje dane dotyczące wpisów w lokalnej pamięci podręcznej DNS podczas wykonywania skanowania IOC (warunek DnsEntryItem).</p> <p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie skanuje lokalnej pamięci podręcznej DNS. Jeśli plik IOC zawiera warunki dokumentu DnsEntryItem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje lokalną pamięć podręczną DNS tylko wtedy, gdy dokument DnsEntryItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p>
<p>/arpentry=on off</p>	<p>Analizuje dane dotyczące wpisów w tabeli ARP podczas wykonywania skanowania IOC (warunek ArpEntryItem).</p> <p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie skanuje tabeli ARP. Jeśli plik IOC zawiera warunki dokumentu ArpEntryItem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje tabelę ARP tylko wtedy, gdy dokument ArpEntryItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p>
<p>/ports=on off</p>	<p>Analizuje dane dotyczące portów otwartych do nasłuchiwania podczas wykonywania skanowania IOC (warunek PortItem).</p> <p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie skanuje tabeli aktywnych połączeń na urządzeniu. Jeśli plik IOC zawiera warunki dokumentu PortItem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje tabelę aktywnych połączeń tylko wtedy, gdy dokument PortItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p>
<p>/services=on off</p>	<p>Analizuje dane dotyczące usług zainstalowanych na urządzeniu podczas wykonywania skanowania IOC (warunek ServiceItem).</p>

	<p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie skanuje danych dotyczących usług zainstalowanych na urządzeniu. Jeśli plik IOC zawiera warunki dokumentu Serviceltem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane usługi tylko wtedy, gdy dokument Serviceltem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p>
/system=on off	<p>Analizuje dane środowiskowe podczas wykonywania skanowania IOC (warunek SystemInfoltem).</p> <p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie analizuje danych środowiskowych. Jeśli plik IOC zawiera warunki dokumentu SystemInfoltem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane środowiskowe tylko wtedy, gdy dokument SystemInfoltem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p>
/users=on off	<p>Analizuje dane dotyczące użytkowników podczas wykonywania skanowania IOC (warunek UserItem).</p> <p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie analizuje danych dotyczących użytkowników utworzonych w systemie. Jeśli plik IOC zawiera warunki dokumentu UserItem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane dotyczące użytkowników tworzonych w systemie tylko wtedy, gdy dokument UserItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p>
/volumes=on off	<p>Analizuje dane dotyczące woluminów podczas wykonywania skanowania IOC (warunek Volumeltem).</p> <p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie skanuje danych dotyczących woluminów na urządzeniu. Jeśli plik IOC zawiera warunki dokumentu Volumeltem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane woluminów tylko wtedy, gdy dokument Volumeltem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p>
/eventlog=on off	<p>Analizuje dane dotyczące wpisów w Dzienniku zdarzeń systemu Windows podczas wykonywania skanowania IOC (warunek EventLogItem).</p> <p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie skanuje wpisów w Dzienniku zdarzeń systemu Windows. Jeśli plik IOC zawiera warunki dokumentu EventLogItem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje Dziennik zdarzeń systemu Windows tylko wtedy, gdy dokument EventLogItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p>
/datetime=<data publikacji zdarzenia>	<p>Należy wziąć pod uwagę datę opublikowania zdarzenia w Dzienniku zdarzeń systemu Windows podczas określania obszaru skanowania</p>

	<p>IOC dla odpowiedniego dokumentu IOC.</p> <p>Podczas wykonywania skanowania IOC, Kaspersky Endpoint Security skanuje wpisy w Dzienniku zdarzeń systemu Windows opublikowane w trakcie czasu od określonej godziny i daty do momentu, gdy zadanie jest uruchomione.</p> <p>Kaspersky Endpoint Security umożliwia określenie daty publikacji zdarzenia jako wartości argumentu. Skanowanie jest wykonywane tylko dla zdarzeń opublikowanych w Dzienniku zdarzeń systemu Windows po określonej dacie, a przed uruchomieniem skanowania.</p> <p>Jeśli argument nie jest określony, Kaspersky Endpoint Security skanuje zdarzenia z dowolną datą publikacji. Ustawienia TaskSettings::BaseSettings::EventLogItem::datetime nie można edytować.</p> <p>Ustawienie jest używane tylko wtedy, gdy dokument EventLogItem IOC został opisany w pliku IOC dostarczonym do przeskanowania.</p>
<p><code>/Channel=<lista kanałów></code></p>	<p>Lista nazw kanałów (dziennik), dla których chcesz wykonać skanowanie IOC.</p> <p>Jeśli argument został określony, Kaspersky Endpoint Security skanuje wpisy opublikowane w określonych dziennikach. Dokument IOC musi zawierać opisany warunek EventLogItem.</p> <p>Nazwa dziennika jest określona jako ciąg znaków zgodnie z nazwą dziennika (kanału), określonego we właściwościach dziennika (parametr Full Name) lub we właściwościach zdarzenia (parametr <Channel></Channel> w schemacie xml zdarzenia). Możesz określić kilka kanałów oddzielonych spacjami.</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security skanuje wpisy dla kanałów Application, System, Security.</p>
<p><code>/files=on off</code></p>	<p>Analizuje dane plików podczas wykonywania skanowania IOC (warunek FileItem).</p> <p>Jeśli wartość argumentu to off, Kaspersky Endpoint Security nie analizuje danych plików. Jeśli plik IOC zawiera warunki dokumentu FileItem IOC, są one ignorowane (wykryte jako brak dopasowania).</p> <p>Jeśli argument nie został określony, Kaspersky Endpoint Security analizuje dane plików tylko wtedy, gdy dokument FileItem IOC został opisany w pliku IOC, dostarczonym do przeskanowania.</p>
<p><code>/drives= <all system critical custom></code></p>	<p>Ustawia obszar skanowania IOC podczas analizowania danych dla dokumentu FileItem IOC.</p> <p>Możesz ustawić następujące wartości dla obszaru skanowania:</p> <ul style="list-style-type: none"> • <all> dla wszystkich dostępnych obszarów plików. • <system> dla plików w folderach, w których zainstalowany jest system operacyjny. • <critical> dla plików tymczasowych w folderach użytkownika i systemowych. • <custom> dla plików w obszarach zdefiniowanych przez użytkownika (/scope=<lista folderów do przeskanowania>). <p>Jeśli argument nie został określony, wykonywanie jest skanowanie obszarów krytycznych.</p>

<code>/excludes=<lista wykluczeń></code>	Ustawia obszar wykluczeń podczas analizowania danych dla dokumentu FileItem IOC. Możesz określić kilka ścieżek oddzielonych spacjami.
<code>/scope=<lista folderów do przeskanowania></code>	Obszar skanowania IOC zdefiniowany przez użytkownika podczas analizowania danych dla dokumentu FileItem IOC (<code>/drives=custom</code>). Możesz określić kilka ścieżek oddzielonych spacjami.

Wartości zwrotne polecenia:

- -1 oznacza, że polecenie nie jest obsługiwane przez wersję Kaspersky Endpoint Agent, który jest zainstalowany na urządzeniu.
- 0 oznacza, że polecenie zostało wykonane pomyślnie.
- 1 oznacza, że obowiązkowy argument nie został przekazany do polecenia.
- 2 oznacza, że wystąpił ogólny błąd.
- 4 oznacza, że wystąpił błąd składniowy.

Jeśli polecenie zostało wykonane pomyślnie (wartość zwrotna 0) i wykryto wskaźniki naruszeń bezpieczeństwa, Kaspersky Endpoint Security zwróci do wiersza poleceń następujące informacje o wyniku wykonania zadania:

Uuid	ID pliku IOC z nagłówka struktury pliku IOC (znacznik <code><ioc id=""></code>)
Nazwa	Opis pliku IOC z nagłówka struktury pliku IOC (znacznik <code><description></code> <code></description></code>)
Dopasowane elementy wskaźnika	Lista identyfikatorów wszystkich dopasowanych wskaźników.
Dopasowane obiekty	Dana każdego dokumentu IOC, dla których było dopasowanie.

MDRLICENSE. Aktywacja MDR

Wykonaj działania na pliku konfiguracyjnym BLOB, aby aktywować Managed Detection and Response. Plik BLOB zawiera ID klienta oraz informacje o licencji dla Kaspersky Managed Detection and Response. Plik BLOB znajduje się w archiwum ZIP pliku konfiguracyjnego MDR. Archiwum ZIP możesz uzyskać w Kaspersky Managed Detection and Response Console. Więcej informacji o pliku BLOB *można znaleźć w [pomocy dla Kaspersky Managed Detection and Response](#)*.

Uprawnienia administratora są wymagane do wykonania działań na pliku BLOB. Ustawienia Managed Detection and Response w zasadzie muszą być także dostępne do edycji (🔑).

Składnia polecenia

```
MDRLICENSE <działanie> [/login=<nazwa użytkownika> /password=<hasło>]
```

Działanie	
<code>/ADD</code> <code><nazwa</code>	Zastosuj plik konfiguracyjny BLOB do integracji z Kaspersky Managed Detection and Response (format pliku P7). Możesz zastosować tylko jeden plik BLOB. Jeśli plik BLOB został już dodany do

pliku>	komputera, plik zostanie zastąpiony.
/DEL	Usuń plik konfiguracyjny BLOB.

Autoryzacja	
/login=<nazwa użytkownika> /password=<hasło>	Dane uwierzytelniające konta użytkownika z żądanymi uprawnieniami Ochrony hasłem .

Na przykład:

- avp.com MDRLICENSE /ADD file.key
- avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1

Kody błędów

Podczas pracy z aplikacją za pośrednictwem wiersza poleceń mogą wystąpić błędy. Jeśli wystąpią błędy, Kaspersky Endpoint Security wyświetla komunikat o błędzie, na przykład, **Błąd: Nie można uruchomić zadania „EntAppControl”**. Kaspersky Endpoint Security może również wyświetlać dodatkowe informacje w postaci kodu, na przykład, **error=8947906D** (patrz tabela poniżej).

Kody błędów

Kod błędu	Opis
09479001	Klucz licencyjny dla Kaspersky Endpoint Security jest już używany na tym komputerze.
0947901D	Licencja utraciła ważność. Aktualizacja bazy danych nie jest dostępna.
89479002	Nie odnaleziono klucza.
89479003	Brak podpisu cyfrowego lub jest on uszkodzony.
89479004	Uszkodzone dane.
89479005	Plik klucza jest uszkodzony.
89479006	Licencja utraciła ważność lub klucz licencyjny utracił ważność.
89479007	Nie określono pliku klucza.
89479008	Nie można zastosować pliku klucza.
89479009	Nie powiodło się zapisanie danych.
8947900A	Nie powiodło się odczytanie danych.
8947900B	Błąd wejścia/wyjścia.
8947900C	Nie odnaleziono baz danych.
8947900E	Biblioteka licencjonowania nie została załadowana.
8947900F	Bazy danych są uszkodzone lub zostały uaktualnione ręcznie.
89479010	Bazy danych są uszkodzone.
89479011	Nie można użyć nieprawidłowego pliku klucza jako klucza zapasowego.
89479012	Błąd systemowy.

89479013	Lista zablokowanych kluczy jest uszkodzona.
89479014	Podpis cyfrowy pliku nie jest zgodny z podpisem cyfrowym Kaspersky.
89479015	Nie można użyć klucza licencji niekomercyjnej jako klucza licencji komercyjnej.
89479016	Aby skorzystać z wersji beta aplikacji, wymagana jest licencja beta.
89479017	Plik klucza nie jest kompatybilny z tą aplikacją.
89479018	Klucz zablokowany przez Kaspersky.
89479019	Obecnie zainstalowana jest wersja testowa aplikacji. Ponowne dodanie testowego klucza licencyjnego nie jest możliwe.
8947901A	Plik klucza jest uszkodzony.
8947901B	Nie odnaleziono podpisu cyfrowego, jest on uszkodzony lub nie jest zgodny z podpisem cyfrowym Kaspersky.
8947901C	Nie można dodać klucza, jeśli odpowiadająca mu licencja niekomercyjna utraciła ważność.
8947901E	Data utworzenia lub aktywacji klucza jest nieprawidłowa. Proszę sprawdzić ustawienia daty systemowej.
8947901F	Nie można dodać klucza licencji testowej: inny klucz licencji testowej jest już aktywny.
89479020	Brak listy zablokowanych kluczy lub jest ona uszkodzona.
89479021	Brak opisu aktualizacji lub jest on uszkodzony.
89479022	Błąd danych usługi klucza licencyjnego.
89479023	Nie można użyć nieprawidłowego pliku klucza jako klucza zapasowego.
89479025	Wystąpił błąd podczas wysyłania żądania do serwera aktywacji. Możliwe przyczyny: błąd połączenia z internetem lub tymczasowe problemy na serwerze aktywacji. Spróbuj aktywować aplikację przy użyciu kodu aktywacyjnego później. Jeżeli problem będzie wciąż występował, skontaktuj się ze swoim dostawcą internetu.
89479026	Błąd odpowiedzi z serwera aktywacyjnego.
89479027	Nie można uzyskać stanu odpowiedzi.
89479028	Wystąpił błąd podczas zapisu pliku tymczasowego.
89479029	Kod aktywacyjny został wpisany niepoprawnie lub data systemowa jest niepoprawna. Sprawdź datę systemową na komputerze.
8947902A	Plik klucza nie jest przeznaczony dla tej aplikacji lub licencja utraciła ważność. Nie możesz aktywować Kaspersky Endpoint Security przy użyciu pliku klucza dla innej aplikacji.
8947902B	Nie powiodło się uzyskanie pliku klucza. Wprowadzono nieprawidłowy kod aktywacyjny.
8947902C	Serwer aktywacji zwrócił błąd 400.
8947902D	Serwer aktywacji zwrócił błąd 401.
8947902E	Serwer aktywacji zwrócił błąd 403.
8947902F	Serwer aktywacji zwrócił błąd 404.
89479030	Serwer aktywacji zwrócił błąd 405.
89479031	Serwer aktywacji zwrócił błąd 406.
89479032	Wymagane jest uwierzytelnienie na serwerze proxy. Sprawdź opcje sieciowe.
89479033	Przekroczono czas oczekiwania na żądanie.

89479034	Serwer aktywacji zwrócił błąd 409.
89479035	Serwer aktywacji zwrócił błąd 410.
89479036	Serwer aktywacji zwrócił błąd 411.
89479037	Serwer aktywacji zwrócił błąd 412.
89479038	Serwer aktywacji zwrócił błąd 413.
89479039	Serwer aktywacji zwrócił błąd 414.
8947903A	Serwer aktywacji zwrócił błąd 415.
8947903C	Błąd wewnętrzny serwera.
8947903D	Funkcja nie jest obsługiwana.
8947903E	Niepoprawna odpowiedź bramy. Sprawdź opcje sieciowe.
8947903F	Usługa niedostępna (błąd HTTP 503).
89479040	Przekroczono czas odpowiedzi bramy. Sprawdź opcje sieciowe.
89479041	Ten protokół nie jest obsługiwany przez serwer.
89479043	Nieznany błąd HTTP.
89479044	Nieprawidłowy identyfikator zasobu.
89479046	Nieprawidłowy adres internetowy.
89479047	Nieprawidłowy folder docelowy.
89479048	Błąd alokacji pamięci.
89479049	Wystąpił błąd podczas konwersji parametrów na ciąg znaków ANSI (adres internetowy, folder, agent).
8947904A	Błąd podczas tworzenia wątku roboczego.
8947904B	Wątek roboczy jest już uruchomiony.
8947904C	Wątek roboczy nie jest uruchomiony.
8947904D	Klucz nie został odnaleziony na serwerze aktywacji.
8947904E	Klucz jest zablokowany.
8947904F	Błąd wewnętrzny na serwerze aktywacji.
89479050	Niewystarczająca ilość informacji w żądaniu aktywacji.
89479053	Klucz licencyjny utracił ważność.
89479054	Na komputerze ustawiono niepoprawną datę systemową.
89479055	Licencja testowa utraciła ważność.
89479056	Licencja utraciła ważność.
89479057	Limit aktywacji określonego kodu aktywacyjnego został przekroczony.
89479058	Procedura aktywacji zakończyła się błędem systemowym.
89479059	Nie można użyć klucza licencji niekomercyjnej jako klucza licencji komercyjnej.
8947905C	Wymagany jest kod aktywacyjny.
89479062	Nie można nawiązać połączenia z serwerem aktywacji.

89479064	Serwer aktywacji jest niedostępny. Proszę sprawdzić połączenie z internetem i ponowić aktywację.
89479065	Data wydania bazy danych aplikacji przekracza datę wygaśnięcia licencji.
89479066	Aktywny klucz nie może zostać zastąpiony kluczem, który utracił swą ważność.
89479067	Nie można dodać klucza zapasowego, jeśli utraci ważność wcześniej niż bieżąca licencja.
89479068	Brak uaktualnionego klucza subskrypcyjnego.
8947906A	Nieprawidłowy kod aktywacyjny (suma kontrolna nie pasuje).
8947906B	Klucz jest już aktywny.
8947906C	Rodzaje licencji odpowiadające kluczowi aktywnemu oraz zapasowemu nie są zgodne.
8947906D	Składnik nie jest obsługiwany przez licencję.
8947906E	Nie można dodać klucza subskrypcyjnego jako klucza zapasowego.
89479213	Ogólny błąd warstwy transportowej.
89479214	Nie można nawiązać połączenia z serwerem aktywacji.
89479215	Nieprawidłowy format adresu internetowego.
89479216	Rozwiązanie adresu serwera proxy nie powiodło się.
89479217	Rozwiązanie adresu serwera nie powiodło się. Proszę sprawdzić ustawienia połączenia z internetem.
89479218	Nie można nawiązać połączenia z serwerem aktywacji lub serwerem proxy.
89479219	Zdalny dostęp zabroniony.
8947921A	Upłynął czas oczekiwania na odpowiedź.
8947921B	Błąd podczas przesyłania żądania HTTP.
8947921C	Błąd połączenia SSL.
8947921D	Operacja przerwana przez wywołanie zwrotne.
8947921E	Zbyt wiele prób przekierowania.
8947921F	Sprawdzenie odbiorcy nie powiodło się.
89479220	Pusta odpowiedź z serwera aktywacji.
89479221	Błąd podczas przesyłania danych.
89479222	Błąd podczas odbierania danych.
89479223	Błąd lokalnego certyfikatu SSL.
89479224	Błąd szyfrowania SSL.
89479225	Błąd certyfikatu SSL serwera.
89479226	Nieprawidłowa zawartość pakietu sieciowego.
89479227	Dostęp użytkownika zabroniony.
89479228	Nieprawidłowy plik certyfikatu SSL.
89479229	Nawiązanie połączenia SSL nie powiodło się.
8947922A	Nie udało się wysłać lub odebrać pakietu sieciowego. Prosimy spróbować ponownie później.

8947922B	Nieprawidłowy plik zawierający unieważnione certyfikaty.
8947922C	Błąd żądania certyfikatu SSL.
89479401	Nieznany błąd serwera.
89479402	Błąd wewnętrzny serwera.
89479403	Brak dostępnego klucza licencyjnego dla wprowadzonego kodu aktywacyjnego.
89479404	Aktywny klucz jest zablokowany.
89479405	Brak wymaganych parametrów żądania aktywacji aplikacji.
89479406	Nieprawidłowa nazwa użytkownika lub hasło.
89479407	Niepoprawny kod aktywacyjny wysłany na serwer.
89479408	Kod aktywacyjny nie jest przeznaczony dla Kaspersky Endpoint Security. Nie możesz aktywować Kaspersky Endpoint Security przy użyciu pliku klucza dla nieznanego programu.
89479409	W żądaniu brakuje kodu aktywacyjnego.
8947940B	Licencja utraciła ważność (zgodnie z danymi z serwera aktywacji).
8947940C	Liczba aktywacji dla tego kodu aktywacyjnego została przekroczona.
8947940D	Nieprawidłowy format żądania ID.
8947940E	Kod aktywacyjny nie jest przeznaczony dla Kaspersky Endpoint Security. Kod aktywacyjny jest przeznaczony dla innego programu Kaspersky.
8947940F	Nie można zaktualizować klucza licencyjnego.
89479410	Kod aktywacyjny nie jest przeznaczony dla tego regionu.
89479411	Kod aktywacyjny nie jest przeznaczony dla wersji językowej Kaspersky Endpoint Security.
89479412	Wymagany jest dodatkowy dostęp do serwera aktywacji.
89479413	Serwer aktywacji zwrócił błąd 643.
89479414	Serwer aktywacji zwrócił błąd 644.
89479415	Serwer aktywacji zwrócił błąd 645.
89479416	Serwer aktywacji zwrócił błąd 646.
89479417	Format kodu aktywacyjnego nie jest obsługiwany przez serwer aktywacji.
89479418	Nieprawidłowy format kodu aktywacyjnego.
89479419	Na komputerze ustawiono niepoprawny czas systemowy.
8947941A	Kod aktywacyjny nie jest przeznaczony dla wersji Kaspersky Endpoint Security.
8947941B	Subskrypcja wygasa:
8947941C	Przekroczono liczbę aktywacji dla tego klucza licencyjnego.
8947941D	Nieprawidłowy podpis cyfrowy klucza licencyjnego.
8947941E	Wymagane są dodatkowe dane.
8947941F	Weryfikacja danych użytkownika nie powiodła się.
89479420	Subskrypcja nieaktywna.
89479421	Trwają prace konserwacyjne serwera aktywacji.

89479501	Nieznany błąd Kaspersky Endpoint Security.
89479502	Przesłano nieprawidłowy parametr. Przykładowo, pustą listę adresów serwerów aktywacji.
89479503	Nieprawidłowy kod aktywacyjny.
89479504	Nieprawidłowa nazwa użytkownika.
89479505	Niepoprawne hasło użytkownika.
89479506	Niepoprawna odpowiedź z serwera aktywacji.
89479507	Prośba o aktywację została przerwana.
89479509	Serwer aktywacji zwrócił pustą listę przekierowań.

Dodatek. Profile aplikacji

Profil to komponent, zadanie lub funkcja Kaspersky Endpoint Security. Profile służą do zarządzania aplikacją z poziomu wiersza poleceń. Za pomocą profili można wykonywać polecenia `START`, `STOP`, `STATUS`, `STATISTICS`, `EXPORT` i `IMPORT`. Korzystając z profili, możesz skonfigurować ustawienia aplikacji (na przykład `STOP DeviceControl`) lub uruchomić zadania (na przykład `START Scan_My_Computer`).

Dostępne są następujące profile:

- `AdaptiveAnomaliesControl` – Adaptacyjna kontrola anomalii.
- `AMSI` – Ochrona AMSI.
- `BehaviorDetection` – Wykrywanie zachowań.
- `DeviceControl` – Kontrola urządzeń.
- `EntAppControl` – Kontrola aplikacji.
- `File_Monitoring` lub `FM` – Ochrona plików.
- `Firewall` lub `FW` – Zapora sieciowa.
- `HIPS` – Ochrona przed włamaniami.
- `IDS` – Ochrona sieci.
- `IntegrityCheck` – Sprawdzanie integralności.
- `Mail_Monitoring` lub `EM` – Ochrona poczty.
- `Rollback` – wycofanie aktualizacji.
- `Scan_ContextScan` – Skanowanie z menu kontekstowego.
- `Scan_IdleScan` – Skanowanie w tle.
- `Scan_Memory` – Skanowanie pamięci jądra.
- `Scan_My_Computer` – Pełne skanowanie.

- Scan_Objects – Skanowanie obiektów.
- Scan_Qscan – Skanowanie obiektów ładowanych podczas uruchamiania systemu operacyjnego.
- Scan_Removable_Drive – Skanowanie dysków wymiennych.
- Scan_Startup lub STARTUP – Skanowanie obszarów krytycznych.
- Updater – Aktualizacja.
- Web_Monitoring lub WM – Ochrona WWW.
- WebControl – Kontrola sieci.

Kaspersky Endpoint Security obsługuje również profile usług. Profile usług mogą być wymagane podczas kontaktu z pomocą techniczną Kaspersky.

Zarządzanie aplikacją za pośrednictwem interfejsu API REST

Kaspersky Endpoint Security umożliwia skonfigurowanie ustawień aplikacji, uruchamianie skanowania, aktualizowanie antywirusowych baz danych i wykonywanie innych zadań przy użyciu rozwiązań innych firm. Kaspersky Endpoint Security oferuje w tym celu interfejs API. Interfejs API REST Kaspersky Endpoint Security działa przez HTTP i składa się z zestawu metod żądania / odpowiedzi. Innymi słowy, możesz zarządzać Kaspersky Endpoint Security za pomocą rozwiązania innej firmy, a nie lokalnego interfejsu aplikacji lub Konsoli administracyjnej Kaspersky Security Center.

Aby rozpocząć korzystanie z interfejsu API REST, musisz [zainstalować Kaspersky Endpoint Security z obsługą interfejsu API REST](#). Klient REST i Kaspersky Endpoint Security muszą być zainstalowani na tym samym komputerze.

W celu zapewnienia bezpiecznej interakcji między Kaspersky Endpoint Security a klientem REST:

- Skonfiguruj ochronę klienta REST przed nieautoryzowanym dostępem zgodnie z zaleceniami dewelopera klienta REST. Skonfiguruj ochronę folder klienta REST przed pracą z pomocą Discretionary Access Control List – DACL.
- Aby uruchomić klienta REST, użyj oddzielnego konta z uprawnieniami administratora. Zablokuj interaktywne logowanie do systemu dla tego konta.

Aplikacja jest zarządzana za pomocą interfejsu API REST pod adresem `http://127.0.0.1` lub `http://localhost`. Zdalne zarządzanie Kaspersky Endpoint Security za pośrednictwem interfejsu API REST nie jest możliwe.

 [OTWÓRZ DOKUMENTACJĘ API REST](#)

Instalowanie aplikacji za pośrednictwem interfejsu API REST

Aby zarządzać aplikacją poprzez interfejs API REST, musisz zainstalować Kaspersky Endpoint Security z obsługą interfejsu API REST. Jeśli zarządzasz Kaspersky Endpoint Security za pośrednictwem interfejsu API REST, nie możesz zarządzać aplikacją za pomocą Kaspersky Security Center.

Przygotowywanie do zainstalowania aplikacji z obsługą API REST

Bezpieczna interakcja Kaspersky Endpoint Security z klientem REST wymaga skonfigurowania identyfikacji żądania. W tym celu należy zainstalować certyfikat i podpisać ładunek każdego żądania.

Aby utworzyć certyfikat, możesz użyć, na przykład, OpenSSL.

Na przykład:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

Użyj algorytmu szyfrowania RSA z kluczem o efektywnej długości wynoszącej 2048 bitów lub więcej.

W rezultacie otrzymasz certyfikat `cert.pem` i klucz prywatny `key.pem`.

Instalowanie aplikacji z obsługą API REST

W celu zainstalowania Kaspersky Endpoint Security z obsługą API REST:

1. Uruchom wiersz poleceń (cmd.exe) jako administrator.
2. Przejdź do folderu zawierającego pakiet dystrybucyjny dla Kaspersky Endpoint Security w wersji 11.2.0 lub nowszej.
3. Zainstaluj Kaspersky Endpoint Security z następującymi ustawieniami:

- RESTAPI=1

- RESTAPI_User=<Nazwa użytkownika>

Nazwa użytkownika do zarządzania aplikacją za pośrednictwem interfejsu API REST. Wpisz nazwę użytkownika w formacie <DOMAIN>\<UserName> (na przykład: RESTAPI_User=COMPANY\Administrator). Aplikację można zarządzać za pośrednictwem interfejsu API REST tylko na tym koncie. Możesz wybrać tylko jednego użytkownika do pracy z interfejsem API REST.

- RESTAPI_Port=<Port>

Port używany do wymiany danych. Jest to parametr opcjonalny. Domyślnie wybrany jest port 6782.

- RESTAPI_Certificate=<ścieżka do certyfikatu>

Certyfikat do identyfikowania żądań (na przykład, RESTAPI_Certificate=C:\cert.pem).

Możesz zainstalować certyfikat po zainstalowaniu aplikacji lub aktualizacji certyfikatu po wygaśnięciu certyfikatu.

[Jak zainstalować certyfikat dla identyfikacji żądania API REST?](#)

1. Wyłącz [Autoochronę Kaspersky Endpoint Security](#)

Mechanizm autoochrony uniemożliwia modyfikowanie i usuwanie plików aplikacji, procesów w pamięci i wpisów w rejestrze systemu.

2. Przejdź do klucza rejestru, który zawiera ustawienia API REST:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\Rest

3. Wprowadź ścieżkę do certyfikatu, na przykład, Certificate = C:\Folder\cert.pem.

4. Włącz [Autoochronę Kaspersky Endpoint Security](#).

5. [Uruchom aplikację ponownie](#).

- AdminKitConnector=1

Zarządzanie aplikacjami za pomocą systemów administracyjnych. Domyślnie zarządzanie jest dozwolone.

Możesz także użyć [pliku setup.ini](#), aby zdefiniować ustawienia do pracy z interfejsem API REST.

Na przykład:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1  
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator  
/pRESTAPI_Certificate=C:\cert.pem /s
```

Dzięki temu będziesz mógł zarządzać aplikacją za pośrednictwem interfejsu API REST. Aby zweryfikować jego działanie, otwórz dokumentację interfejsu API REST za pomocą żądania GET.

Na przykład:

```
GET http://localhost:6782/kes/v1/api-docs
```

Jeśli zainstalowałeś aplikację z obsługą API REST, Kaspersky Endpoint Security automatycznie tworzy regułę zezwalającą w ustawieniach Kontroli sieci do uzyskania dostępu do zasobów sieciowych (*reguła usługowa dla REST API*). Ta reguła jest potrzebna, aby zezwolić klientowi REST na dostęp do Kaspersky Endpoint Security przez cały czas. Na przykład, jeśli ograniczyłeś dostęp użytkownika do zasobów sieciowych, to nie będzie wpływało na zarządzanie aplikacją poprzez API REST. Zalecane jest, żebyś nie usuwał reguły lub nie zmieniał ustawień *reguły usługowej dla API REST*. Jeśli usunąłeś regułę, Kaspersky Endpoint Security przywróci ją po ponownym uruchomieniu aplikacji.

Praca z interfejsem API

Nie można ograniczyć dostępu do aplikacji za pośrednictwem interfejsu API REST za pomocą [Ochrony hasłem](#). Na przykład nie można zablokować użytkownikowi możliwości wyłączenia ochrony za pośrednictwem interfejsu API REST. Możesz skonfigurować Ochronę hasłem za pośrednictwem interfejsu API REST i ograniczyć dostęp użytkownika do aplikacji za pośrednictwem interfejsu lokalnego.

Aby zarządzać aplikacją za pośrednictwem interfejsu API REST, musisz uruchomić klienta REST na koncie określonym podczas [instalowania aplikacji z obsługą interfejsu API REST](#). Możesz wybrać tylko jednego użytkownika do pracy z interfejsem API REST.



[OTWÓRZ DOKUMENTACJĘ API REST](#)

Zarządzanie aplikacją za pośrednictwem interfejsu API REST obejmuje następujące kroki:

1. Uzyskanie aktualnych wartości ustawień aplikacji. Aby to zrobić, wyślij żądanie GET.

Na przykład:

```
GET http://localhost:6782/kes/v1/settings/ExploitPrevention
```

2. Aplikacja wyśle odpowiedź ze strukturą i wartościami ustawień. Kaspersky Endpoint Security obsługuje formaty XML i JSON.

Na przykład:

```
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": true,
  "enabled": true
}
```

3. Zmodyfikuj ustawienia aplikacji. Użyj struktury ustawień otrzymanej w odpowiedzi na żądanie GET.

Na przykład:

```
{
  "action": 0,
  "enableSystemProcessesMemoryProtection": false,
  "enabled": true
}
```

4. Zapisz ustawienia aplikacji (ładunek) w JSON (payload.json).

5. Zapisz JSON w formacie PKCS7.

Na przykład:

```
$ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out signed_payload.pem
```

W rezultacie uzyskasz podpisany plik z ładunkiem żądania (`signed_payload.pem`).

6. Zmodyfikuj ustawienia aplikacji. Aby to zrobić, wyślij żądanie POST i załącz podpisany plik z ładunkiem żądania (`signed_payload.pem`).

Aplikacja stosuje nowe ustawienia i wysyła odpowiedź zawierającą wyniki konfiguracji aplikacji (odpowiedź może być pusta). Możesz sprawdzić, czy ustawienia są aktualizowane przy użyciu żądania GET.

Źródła informacji o aplikacji

Strona programu Kaspersky Endpoint Security na witrynie Kaspersky

Na [stronie Kaspersky Endpoint Security](#) znajdziesz ogólne informacje o aplikacji, jej funkcjach i właściwościach.

Strona Kaspersky Endpoint Security zawiera odsyłacz do sklepu internetowego. Możesz w nim kupić lub odnowić licencję dla aplikacji.

Strona Kaspersky Endpoint Security w Bazie Wiedzy

Baza wiedzy to sekcja na stronie działu pomocy technicznej.

Na [stronie Kaspersky Endpoint Security w Bazie wiedzy](#) znajdują się artykuły zawierające przydatne informacje, zalecenia i odpowiedzi na najczęściej zadawane pytania dotyczące zakupu, instalacji i korzystania z aplikacji.

Artykuły mogą zawierać odpowiedzi na pytania spoza zakresu programu Kaspersky Endpoint Security, związane z innymi aplikacjami Kaspersky. Mogą one także zawierać nowości z działu pomocy technicznej.

Dyskusja na temat aplikacji Kaspersky w społeczności użytkowników

Jeżeli zapytanie nie wymaga natychmiastowej odpowiedzi, można przedyskutować je z ekspertami z firmy Kaspersky lub innymi użytkownikami jej oprogramowania na stronie [Społeczności](#).

Na stronie Społeczności możesz przeglądać istniejące tematy, pozostawiać swoje komentarze i tworzyć nowe tematy.

Kontakt z działem pomocy technicznej

Jeśli nie znajdziesz rozwiązania swojego problemu w dokumentacji lub w innych [źródłach informacji o Kaspersky Endpoint Security](#), zalecamy skontaktować się z działem pomocy technicznej. Eksperti z działu pomocy technicznej odpowiedzą na Twoje pytania związane z instalacją i użytkowaniem Kaspersky Endpoint Security.

Kaspersky oferuje wsparcie dla Kaspersky Endpoint Security podczas cyklu życia aplikacji (zapoznaj się ze [stroną cyklu życia aplikacji](#)). Przed skontaktowaniem się z działem pomocy technicznej przeczytaj [zasady korzystania z pomocy technicznej](#).

Możesz skontaktować się z działem pomocy technicznej na jeden z następujących sposobów:

- [Odwiedzając stronę pomocy technicznej](#)
- Wysyłając zgłoszenie do pomocy technicznej poprzez [portal Kaspersky CompanyAccount](#)

Po poinformowaniu o swoim problemie specjalistów z działu pomocy technicznej Kaspersky, mogą oni poprosić o utworzenie *pliku śledzenia*. Plik śledzenia umożliwia śledzenie procesu wykonywania poleceń aplikacji krok po kroku, a także określenie etapu działania aplikacji, w którym pojawił się błąd.

Specjaliści z pomocy technicznej mogą również potrzebować dodatkowych informacji o systemie operacyjnym, uruchomionych na komputerze procesach, szczegółowego raportu z działania modułów aplikacji.

Podczas wykonywania diagnostyki specjaliści z działu pomocy technicznej mogą poprosić o zmianę ustawień aplikacji poprzez:

- Aktywowanie funkcji gromadzenia rozszerzonych informacji diagnostycznych.
- Dostosowanie ustawień pojedynczych komponentów aplikacji, które nie są dostępne poprzez elementy standardowego interfejsu użytkownika.
- Zmianę ustawień przechowywania informacji diagnostycznych.
- Konfigurację przechwytywania i rejestrowania ruchu sieciowego.

Eksperti z pomocy technicznej dostarczą wszystkie informacje potrzebne do wykonania tych działań (opis sekwencji kroków, ustawienia, które mają zostać zmodyfikowane, pliki konfiguracyjne, skrypty, dodatkowe funkcje wiersza polecenia, moduły diagnostyczne, narzędzia do zadań specjalnych itd.) oraz poinformują o zakresie danych używanych w celach diagnostycznych. Rozszerzone informacje diagnostyczne są zapisywane na komputerze użytkownika. Dane nie są automatycznie przesyłane do Kaspersky.

Powyższe działania powinny być wykonywane tylko pod nadzorem specjalistów z pomocy technicznej i zgodnie z ich poleceniami. Wykonywanie nienadzorowanych zmian w ustawieniach aplikacji w sposób inny niż ten opisany w Podręczniku administratora lub przez specjalistów z pomocy technicznej może spowolnić lub zawiesić system operacyjny, wpłynąć na ochronę komputera lub zaburzyć dostępność i integralność przetwarzanych danych.

Zawartość i przechowywanie plików śledzenia

Jesteś osobiście odpowiedzialny za bezpieczeństwo danych przechowywanych na swoim komputerze, w szczególności za monitorowanie i ograniczanie dostępu do danych, aż do momentu wysłania ich do Kaspersky.

Pliki śledzenia są przechowywane na komputerze tak długo, jak aplikacja jest używana i są trwale usuwane, gdy aplikacja jest usuwana.

Pliki śledzenia, za wyjątkiem plików śledzenia Agenta autoryzacji, są przechowywane w folderze %ProgramData%\Kaspersky Lab\KES\Traces.

Nazwy są nadawane plikom śledzenia w następujący sposób: KES<numer wersji usługi_dataXX.XX_godzinaXX.XX_pidXXX.><typ pliku śledzenia>.log.

Możesz przejrzeć dane zapisane w plikach śledzenia.

Wszystkie pliki śledzenia zawierają następujące dane:

- Czas zdarzenia.
- Liczbę procesów wykonania.

Plik śledzenia Agenta autoryzacji nie zawiera tej informacji.

- Komponent aplikacji, który wywołał zdarzenie.
- Poziom priorytetu zdarzenia (zdarzenie informacyjne, ostrzeżenie, zdarzenie krytyczne, błąd).
- Opis zdarzenia dotyczący wykonania polecenia przez moduł aplikacji oraz wynik wykonania tego polecenia.

Kaspersky Endpoint Security zapisuje hasła użytkownika do pliku śledzenia tylko w postaci zaszyfrowanej.

Zawartość plików śledzenia SRV.log, GUI.log oraz ALL.log

Oprócz ogólnych danych, pliki śledzenia SRV.log, GUI.log i ALL.log mogą przechowywać następujące informacje:

- Dane osobowe, łącznie z nazwiskiem, imieniem oraz drugim imieniem, jeśli takie dane są uwzględnione w ścieżce dostępu do plików na komputerze lokalnym.
- Dane dotyczące sprzętu zainstalowanego na komputerze (takie jak dane oprogramowania układowego BIOS/UEFI). Te dane są zapisywane w celu zapisu do plików śledzenia podczas przeprowadzania Kaspersky Disk Encryption.
- Nazwa użytkownika i hasło, jeśli były otwarcie przesyłane. Dane te mogą być zapisywane w plikach śledzenia podczas skanowania ruchu internetowego.
- Nazwa użytkownika i hasło, jeśli znajdują się w nagłówkach HTTP.
- Nazwa konta Microsoft Windows, jeśli nazwa konta jest uwzględniona w nazwie pliku.
- Twój adres e-mail lub adres sieciowy zawierający nazwę Twojego konta i hasło, jeśli znajdują się w nazwie wykrytego obiektu.

- Odwiedzane strony internetowe oraz przekierowania z tych stron. Dane te są zapisywane w plikach śledzenia, gdy aplikacja skanuje strony internetowe.
- Adres serwera proxy, nazwa komputera, port, adres IP i login używany przy dostępie do serwera proxy. Dane te są zapisywane w plikach śledzenia, jeśli aplikacja używa serwera proxy.
- Zdalne adresy IP, z którymi Twój komputer nawiązał połączenie.
- Temat wiadomości, numer ID, adres i nazwisko nadawcy wiadomości, strona internetowa nadawcy w sieci społecznościowej. Dane te są zapisywane w plikach śledzenia, jeśli Kontrola sieci jest włączona.
- Dane dotyczące ruchu sieciowego. Dane są zapisywane w plikach śledzenia, jeśli włączone są komponenty monitorowania ruchu (takie jak Kontrola sieci).
- Dane otrzymane z serwerów Kaspersky (takie jak wersja antywirusowych baz danych).
- Stany składników Kaspersky Endpoint Security i dane dotyczące ich działania.
- Dane dotyczące aktywności użytkownika w aplikacji.
- Zdarzenia systemu operacyjnego.

Zawartość plików śledzenia HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Poza ogólnymi danymi, plik śledzenia HST .log zawiera informacje o wykonaniu zadania aktualizacji bazy danych i modułów aplikacji.

Oprócz ogólnych danych, plik śledzenia BL .log zawiera informacje o zdarzeniach występujących podczas działania aplikacji, a także o danych wymaganych do rozwiązania błędów aplikacji. Ten plik jest tworzony, jeśli aplikacja jest uruchamiana w parametrem avp.exe -bl.

Plik śledzenia Dumpwriter .log zawiera nie tylko ogólne dane, ale także informacje o usłudze niezbędne do rozwiązania problemów występujących podczas zapisywania plików zrzutu pamięci aplikacji.

Poza ogólnymi danymi, plik śledzenia WD .log zawiera informacje o zdarzeniach występujących podczas działania usługi avpsus, w tym o zdarzeniach aktualizacji modułów aplikacji.

Plik śledzenia AVPCon .dll .log zawiera nie tylko ogólne dane, ale także informacje o zdarzeniach występujących podczas działania modułu połączeniowego Kaspersky Security Center.

Zawartość plików śledzenia wydajności

Nazwy są nadawane plikom śledzenia wydajności w następujący sposób: KES<numer wersji_dataXX.XX_godzinaXX.XX_pidXXX.>PERF.HAND.etl.

Oprócz ogólnych danych, pliki śledzenia wydajności zawierają informacje o obciążeniu procesora, informacje o czasie ładowania systemu operacyjnego i aplikacji, a także informacje o uruchomionych procesach.

Zawartość plików śledzenia modułu Ochrona AMSI

Oprócz ogólnych danych, plik śledzenia AMSI.log zawiera informacje o wynikach skanowania wykonanego na żądanie ze strony aplikacji firm trzecich.

Zawartości plików śledzenia komponentu Ochrona poczty

Oprócz ogólnych danych, plik śledzenia `mcou.OUTLOOK.EXE.log` może zawierać części wiadomości e-mail, w tym adresy e-mail.

Zawartości plików śledzenia komponentu Skanowanie z menu kontekstowego

Oprócz ogólnych informacji, plik śledzenia `shelllex.dll.log` zawiera informacje o zakończeniu zadania skanowania i danych wymaganych do debugowania aplikacji.

Zawartość plików śledzenia wtyczki webowej aplikacji

Pliki śledzenia wtyczki webowej aplikacji są przechowywane na komputerze, na którym wdrożono Kaspersky Security Center Web Console, w folderze `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs`.

Pliki śledzenia wtyczki webowej aplikacji mają następujące nazwy: `logs-kes_windows-<typ pliku śledzenia>.DESKTOP-<data aktualizacji pliku>.log`. Konsola Web Console rozpoczyna zapisywanie danych po instalacji, a usuwanie plików śledzenia po usunięciu Web Console.

Pliki śledzenia wtyczki webowej aplikacji zawierają nie tylko ogólne dane, ale także następujące informacje:

- Hasło użytkownika KLAdmin do odblokowania interfejsu Kaspersky Endpoint Security ([Ochrona hasłem](#)).
- Tymczasowe hasło do odblokowania interfejsu Kaspersky Endpoint Security ([Ochrona hasłem](#)).
- Nazwa użytkownika i hasło dla serwera pocztowego SMTP ([Powiadomienia e-mail](#)).
- Nazwa użytkownika i hasło dla internetowego serwera proxy ([Serwer proxy](#)).
- Nazwa użytkownika i hasło dla [zadania Zmiana składników aplikacji](#).
- Dane uwierzytelniające i ścieżki określone w zadaniach i właściwościach profilu Kaspersky Endpoint Security.

Zawartość pliku śledzenia Agenta autoryzacji

Plik śledzenia Agenta autoryzacji jest przechowywany w folderze informacji o woluminie systemowym i posiada następującą nazwę: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Oprócz ogólnych danych, plik śledzenia Agenta autoryzacji zawiera informacje o działaniu Agenta autoryzacji oraz o działaniach wykonywanych przez użytkownika na Agencie autoryzacji.

Śledzenie działania aplikacji

Śledzenie aplikacji to szczegółowy zapis akcji, wykonanych przez aplikację, oraz wiadomości o zdarzeniach, które wystąpiły w trakcie działania aplikacji.

Śledzenie aplikacji powinno odbywać się pod nadzorem pomocy technicznej Kaspersky.

W celu utworzenia pliku śledzenia aplikacji:

1. W oknie głównym aplikacji kliknij przycisk .

Zostanie otwarte okno **Pomoc techniczna**.

2. W oknie **Pomoc techniczna** kliknij przycisk **Narzędzia pomocy technicznej**.

3. Użyj przełącznika **Włącz śledzenie aplikacji**, aby włączyć lub wyłączyć śledzenie działania aplikacji.

4. Z listy rozwijalnej **Śledzenie** wybierz tryb śledzenia aplikacji:

- **Z rotacją**. Zapisuje ślady do ograniczonej liczby plików o ograniczonym rozmiarze i nadpisuje starsze pliki po osiągnięciu maksymalnego rozmiaru. Jeśli ten tryb jest zaznaczony, możesz zdefiniować maksymalną liczbę plików dla rotacji oraz maksymalny rozmiar dla każdego pliku.

- **Zapisz do pojedynczego pliku**. Zapisuje jeden plik śledzenia (bez ograniczenia rozmiaru).

5. Z listy rozwijalnej **Poziom** wybierz poziom śledzenia.

Zaleca się uzgodnić wymagany poziom śledzenia ze specjalistami z pomocy technicznej. Jeżeli z pomocy technicznej nie zostały przekazane żadne zalecenia, należy ustawić poziom śledzenia na **Normalny (500)**.

6. Uruchom ponownie Kaspersky Endpoint Security.

7. Aby zatrzymać proces śledzenia, wróć do okna **Pomoc techniczna** i wyłącz śledzenie.

Pliki śledzenia możesz także utworzyć podczas instalowania aplikacji z poziomu [wiersza poleceń](#), w tym przy użyciu [pliku setup.ini](#).

W rezultacie plik śledzenia zostanie utworzony w folderze %ProgramData%\Kaspersky Lab\KES\Traces. Po utworzeniu pliku śledzenia, wyślij plik do pomocy technicznej Kaspersky.

Kaspersky Endpoint Security automatycznie usuwa pliki śledzenia podczas usuwania aplikacji. Możliwe jest również ręczne usunięcie tych plików. W tym celu należy włączyć śledzenie i [zatrzymać działanie aplikacji](#).

Śledzenie wydajności aplikacji

Kaspersky Endpoint Security umożliwia otrzymywanie informacji o problemach z działaniem komputera podczas korzystania z aplikacji. Na przykład, możesz otrzymywać informacje o opóźnieniach w ładowaniu systemu operacyjnego po zainstalowaniu aplikacji. Aby to zrobić, Kaspersky Endpoint Security tworzy [pliki śledzenia wydajności](#). *Śledzenie wydajności* odnosi się do rejestrowania działań wykonanych przez aplikację w celu zdiagnozowania problemów z działaniem Kaspersky Endpoint Security. Aby otrzymywać informacje, Kaspersky Endpoint Security używa usługi Śledzenie zdarzeń systemu Windows (ETW). Pomoc techniczna Kaspersky jest odpowiedzialna za diagnozowanie problemów z Kaspersky Endpoint Security i znalezienie powodów tych problemów.

Śledzenie aplikacji powinno odbywać się pod nadzorem pomocy technicznej Kaspersky.

W celu utworzenia pliku śledzenia wydajności:

1. W oknie głównym aplikacji kliknij przycisk .

Zostanie otwarte okno **Pomoc techniczna**.

2. W oknie **Pomoc techniczna** kliknij przycisk **Narzędzia pomocy technicznej**.
3. Użyj przełącznika **Włącz śledzenie wydajności**, aby włączyć lub wyłączyć śledzenie działania aplikacji.
4. Z listy rozwijalnej **Śledzenie** wybierz tryb śledzenia aplikacji:
 - **Z rotacją**. Zapisuje ślady do ograniczonej liczby plików o ograniczonym rozmiarze i nadpisuje starsze pliki po osiągnięciu maksymalnego rozmiaru. Jeśli ten tryb jest wybrany, możesz zdefiniować maksymalny rozmiar każdego pliku.
 - **Zapisz do pojedynczego pliku**. Zapisuje jeden plik śledzenia (bez ograniczenia rozmiaru).
5. Z listy rozwijalnej **Poziom** wybierz poziom śledzenia:
 - **Niski**. Kaspersky Endpoint Security analizuje najważniejsze procesy systemu operacyjnego związane z działaniem.
 - **Szczegółowy**. Kaspersky Endpoint Security analizuje wszystkie procesy systemu operacyjnego związane z działaniem.
6. Z listy rozwijalnej **Typ śledzenia** wybierz typ śledzenia:
 - **Informacje podstawowe**. Kaspersky Endpoint Security analizuje procesy podczas działania systemu operacyjnego. Użyj tego typu śledzenia, jeśli problem występuje po załadowaniu systemu operacyjnego, takich jak problem z uzyskaniem dostępu do internetu w przeglądarce.
 - **Przy ponownym uruchomieniu**. Kaspersky Endpoint Security analizuje procesy tylko podczas ładowania systemu operacyjnego. Po załadowaniu systemu operacyjnego, Kaspersky Endpoint Security zatrzymuje śledzenie. Użyj tego typu śledzenia, jeśli problem jest związany z opóźnieniem ładowania systemu operacyjnego.
7. Uruchom komputer ponownie i spróbuj odtworzyć problem.
8. Aby zatrzymać proces śledzenia, wróć do okna **Pomoc techniczna** i wyłącz śledzenie.

W rezultacie plik śledzenia zostanie utworzony w folderze %ProgramData%\Kaspersky Lab\KES\Traces. Po utworzeniu pliku śledzenia, wyślij plik do pomocy technicznej Kaspersky.

Zapisywanie zrzutu pamięci

Plik zrzutu pamięci zawiera wszystkie informacje o pamięci roboczej procesów Kaspersky Endpoint Security w momencie utworzenia pliku zrzutu.

Zapisane pliki zrzutów mogą zawierać poufne dane. Aby kontrolować dostęp do danych, musisz niezależnie zapewnić bezpieczeństwo plików zrzutów pamięci.

Pliki zrzutów pamięci są przechowywane na komputerze tak długo, jak aplikacja jest używana i są trwale usuwane, gdy aplikacja jest usuwana. Pliki zrzutów pamięci są przechowywane w folderze %ProgramData%\Kaspersky Lab\KES\Traces.

W celu włączenia lub wyłączenia zapisywania plików zrzutów pamięci:

1. W oknie głównym aplikacji kliknij przycisk .

2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ogólne**.
3. W sekcji **Informacje debugowania** użyj pola **Włącz zapisywanie zrzutów pamięci**, aby włączyć lub wyłączyć zapisywanie zrzutów pamięci aplikacji.
4. Zapisz swoje zmiany.


Ochrona plików zrzutu i plików śledzenia

Pliki zrzutów pamięci oraz pliki śledzenia zawierają informacje o systemie operacyjnym i mogą także zawierać [dane użytkownika](#). Aby zablokować dostęp do tych danych, możesz włączyć ochronę plików zrzutu i plików śledzenia.

Jeśli ochrona plików zrzutu i plików śledzenia jest włączona, dostęp do plików mogą uzyskać następujący użytkownicy:

- Dostęp do plików zrzutu może uzyskać administrator systemowy i administrator lokalny, a także użytkownik, który włączył zapisywanie plików zrzutu pamięci i plików śledzenia.
- Dostęp do plików śledzenia może uzyskać tylko administrator systemowy i administrator lokalny.

W celu włączenia lub wyłączenia ochrony plików zrzutu i plików śledzenia:

1. W oknie głównym aplikacji kliknij przycisk .
2. W oknie ustawień aplikacji wybierz **Ustawienia zaawansowane** → **Ogólne**.
3. W sekcji **Informacje debugowania** użyj pola **Włącz ochronę zrzutów pamięci i plików śledzenia**, aby włączyć lub wyłączyć ochronę plików.
4. Zapisz swoje zmiany.

Pliki zrzutu i pliki śledzenia, które zostały zapisane, gdy ochrona była aktywna, pozostaną chronione nawet po wyłączeniu tej funkcji.

Ograniczenia i uwagi

Kaspersky Endpoint Security posiada kilka ograniczeń, które nie są krytyczne dla działania aplikacji.

[Instalowanie aplikacji](#) 

- Więcej informacji na temat obsługi systemów operacyjnych Microsoft Windows 10, Microsoft Windows Server 2016 i Microsoft Windows Server 2019 można znaleźć w [Bazie wiedzy na stronie działu pomocy technicznej](#).
- Więcej informacji na temat obsługi systemów operacyjnych Microsoft Windows Server 11 i Microsoft Windows Server 2022 można znaleźć w [Bazie wiedzy na stronie działu pomocy technicznej](#).
- Po zainstalowaniu aplikacji na zainfekowanym komputerze, nie informuje ona użytkownika o konieczności przeprowadzenia skanowania. Mogą wystąpić problemy [z aktywacją aplikacji](#). Aby rozwiązać te problemy, [uruchom Skanowanie obszarów krytycznych](#).
- Jeśli w plikach setup.ini i setup.reg używane są znaki inne niż ASCII (na przykład znaki cyrylicy), zalecamy edycję pliku w Notepad.exe i zapisanie go w kodowaniu UTF-16LE. Inne opcje kodowania nie są obsługiwane.
- Aplikacja nie obsługuje znaków innych niż ASCII podczas określania ścieżki instalacji aplikacji w [ustawieniach pakietu instalacyjnego](#).
- Jeśli [ustawienia aplikacji są importowane z pliku CFG](#), wartość ustawienia, które definiuje uczestnictwo w Kaspersky Security Network, nie jest stosowana. Po zaimportowaniu ustawień przeczytaj treść Oświadczenia Kaspersky Security Network i potwierdź zgodę na uczestnictwo w Kaspersky Security Network. Treść Oświadczenia możesz przeczytać w interfejsie aplikacji lub w pliku ksn_*.txt, znajdującym się w folderze zawierającym pakiet dystrybucyjny aplikacji.
- Jeśli chcesz usunąć, a następnie ponownie zainstalować szyfrowanie (FLE lub FDE) lub komponent Kontrola urządzeń, musisz uruchomić system ponownie przed ponowną instalacją.
- Jeśli używasz systemu operacyjnego Microsoft Windows 10, po usunięciu komponentu Szyfrowanie plików (FLE) musisz uruchomić system ponownie.
- Podczas próby zainstalowania dowolnej wersji Modułu szyfrującego AES na komputerze, na którym jest zainstalowany program Kaspersky Endpoint Security for Windows 11.7.0, ale nie ma zainstalowanych komponentów szyfrowania, instalacja Modułu szyfrującego zakończy się błędem z informacją, że zainstalowana jest nowsza wersja aplikacji. Począwszy od wersji Kaspersky Endpoint Security 10 for Windows Service Pack 2 (wersja 10.3.0.6294), nie istnieje oddzielny plik instalacyjny dla Modułu szyfrującego. Biblioteki szyfrowania są zawarte w pakiecie dystrybucyjnym aplikacji. Kaspersky Endpoint Security 11.7.0 jest niekompatybilny z modułami szyfrowania AES. Biblioteki wymagane do szyfrowania są instalowane automatycznie po wybraniu komponentu Szyfrowanie całego dysku (FDE) lub Szyfrowanie plików (FLE).
- Instalacja aplikacji może zakończyć się błędem stwierdzającym, że *na komputerze została zainstalowana aplikacja bez nazwy lub z nazwą, która jest nieczytelna*. To oznacza, że na komputerze pozostają niekompatybilne aplikacje lub ich fragmenty. Aby usunąć artefakty lub niekompatybilne aplikacje, wyślij zgłoszenie ze szczegółowym opisem sytuacji do pomocy technicznej Kaspersky za pośrednictwem [Kaspersky CompanyAccount](#).
- Jeśli anulowałeś usunięcie aplikacji, po ponownym uruchomieniu komputera uruchom jej odzyskiwanie.
- Na komputerach działających pod kontrolą systemu Windows 10 w wersji 1903 i 1909, aktualizacje z Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (wersja 10.3.3.275), Service Pack 2 Maintenance Release 4 (wersja 10.3.3.304), 11.0.0 i 11.0.1 z zainstalowanym komponentem Szyfrowanie plików (FLE) może zakończyć się błędem. Jest to spowodowane tym, że w systemie Windows 10 w wersji 1903 i 1909 szyfrowanie plików nie jest obsługiwane dla tych wersji Kaspersky Endpoint Security for Windows. Przed zainstalowaniem tej aktualizacji zalecane jest [usunięcie komponentu szyfrowania plików](#).
- Aplikacja wymaga programu Microsoft .NET Framework 4.0 lub nowszego. Microsoft .NET Framework 4.6.1 posiada luki. Jeśli używasz Microsoft .NET Framework 4.6.1, musisz zainstalować aktualizacje zabezpieczeń.

Więcej informacji o aktualizacjach zabezpieczeń Microsoft .NET Framework możesz znaleźć na [stronie internetowej pomocy technicznej firmy Microsoft](#).

- Jeśli aktualizujesz poprzednią wersję aplikacji do wersji 11.7.0, aby zainstalować Kaspersky Endpoint Agent, uruchom komputer ponownie i zaloguj się do systemu, korzystając z konta z uprawnieniami administratora lokalnego. W przeciwnym razie program Kaspersky Endpoint Agent nie zostanie zainstalowany podczas procedury aktualizacji.
- Jeśli aplikacja została niepomyślnie zainstalowana z komponentem Kaspersky Endpoint Agent wybranym w serwerowym systemie operacyjnym i zostało wyświetlone okno *Błąd Koordynatora Instalatora Windows*, zapoznaj się z instrukcjami na stronie internetowej pomocy technicznej firmy Microsoft.
- Jeśli aplikacja została zainstalowana lokalnie w trybie nieinteraktywnym, użyj udostępnionego [pliku setup.ini](#), aby zastąpić zainstalowane komponenty.
- Po zainstalowaniu programu Kaspersky Endpoint Security for Windows w niektórych konfiguracjach Windows 7, Windows Defender będzie dalej działać. Aby zapobiec obniżeniu wydajności systemu, zalecane jest ręczne wyłączenie Windows Defender.

[Aktualizowanie aplikacji](#)

- Podczas aktualizowania z Kaspersky Endpoint Security 10 Service Pack 2 for Windows (wersja 10.3.0.6294) [zostaje włączony komponent Ochrona przed włamaniami](#).
- Podczas aktualizacji Kaspersky Endpoint Security 10 for Windows Service Pack 2 (wersja 10.3.0.6294), pliki, które w poprzedniej wersji aplikacji zostały umieszczone w Kopii zapasowej lub Kwarantannie, zostaną przeniesione do Kopii zapasowej w nowej wersji aplikacji. Te pliki nie są przesyłane dla wersji wcześniejszych niż Kaspersky Endpoint Security 10 for Windows Service Pack 2 (wersja 10.3.0.6294). Aby je zapisać, należy przywrócić pliki z Kwarantanny i Kopii zapasowej przed zaktualizowaniem aplikacji. Po zakończeniu aktualizacji, ponownie przeskanuj przywrócone pliki.
- Począwszy od wersji 11.0.0, możesz zainstalować wtyczkę MMC Kaspersky Endpoint Security for Windows na poprzedniej wersji wtyczki. Aby wrócić do poprzedniej wersji wtyczki, usuń bieżącą wersję wtyczki i zainstaluj poprzednią wersję wtyczki.
- Podczas aktualizowania Kaspersky Endpoint Security 11.0.0 lub 11.0.1 for Windows, [ustawienia terminarza dla lokalnego zadania aktualizacji, skanowania obszarów krytycznych, skanowania niestandardowego i sprawdzania integralności](#) nie są zapisywane.
- Na komputerach działających pod kontrolą systemu Windows 10 w wersji 1903 i 1909, aktualizacje z Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (wersja 10.3.3.275), Service Pack 2 Maintenance Release 4 (wersja 10.3.3.304), 11.0.0 i 11.0.1 z zainstalowanym komponentem Szyfrowanie plików (FLE) może zakończyć się błędem. Jest to spowodowane tym, że w systemie Windows 10 w wersji 1903 i 1909 szyfrowanie plików nie jest obsługiwane dla tych wersji Kaspersky Endpoint Security for Windows. Przed zainstalowaniem tej aktualizacji zalecane jest [usunięcie komponentu szyfrowania plików](#).
- Aplikacja wymaga programu Microsoft .NET Framework 4.0 lub nowszego. Microsoft .NET Framework 4.6.1 posiada luki. Jeśli używasz Microsoft .NET Framework 4.6.1, musisz zainstalować aktualizacje zabezpieczeń. Więcej informacji o aktualizacjach zabezpieczeń Microsoft .NET Framework możesz znaleźć na [stronie internetowej pomocy technicznej firmy Microsoft](#).
- Jeśli aktualizujesz poprzednią wersję aplikacji do wersji 11.7.0, aby zainstalować Kaspersky Endpoint Agent, uruchom komputer ponownie i zaloguj się do systemu, korzystając z konta z uprawnieniami administratora lokalnego. W przeciwnym razie program Kaspersky Endpoint Agent nie zostanie zainstalowany podczas procedury aktualizacji.
- Jeśli aktualizujesz Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 4 z zainstalowanym komponentem Szyfrowanie plików (FLE) na komputerach działających pod kontrolą systemu Windows 10 w wersji 1809, 1903 i 1909, sterowniki FDE nie będą instalowane do obrazu WinRE.
- Jeśli aktualizujesz Kaspersky Endpoint Security, aplikacja wyłącza korzystanie z KSN, dopóki nie zaakceptujesz Oświadczenia Kaspersky Security Network. Dodatkowo, stan komputera może zostać zmieniony na *Krytyczny* w Kaspersky Security Center; zostanie odebrane zdarzenie *serwery KSN są niedostępne*. Jeśli używasz [Kaspersky Managed Detection and Response](#), otrzymasz zdarzenia dotyczące naruszeń związanych z działaniem rozwiązania. Użycie KSN jest wymagane do działania Kaspersky Managed Detection and Response. Kaspersky Endpoint Security [włącza użycie KSN](#) po zastosowaniu zasady, w której administrator akceptuje warunki korzystania z KSN. Po zaakceptowaniu Oświadczenia Kaspersky Security Network, Kaspersky Endpoint Security wznowia jego działanie.
- Po zaktualizowaniu aplikacji z wersji wcześniejszych niż Kaspersky Endpoint Security 11 for Windows, komputer musi być uruchomiony ponownie.

- System plików ReFS jest obsługiwany z ograniczeniami:
 - Kaspersky Endpoint Security może niepoprawnie przetwarzać zdarzenia dotyczące leczenia zagrożeń. Na przykład, jeśli aplikacja usunęła szkodliwy plik, raport może zawierać wpis *Obiekt nie został przetworzony*. W tym samym czasie Kaspersky Endpoint Security wyleczy zagrożenia zgodnie z ustawieniami aplikacji. Kaspersky Endpoint Security może także zduplikować zdarzenie *Obiekt zostanie wyleczony po ponownym uruchomieniu* dla tego samego obiektu.
 - Ochrona plików może pominąć niektóre zagrożenia. W tym samym czasie Skanowanie antywirusowe działa poprawnie.
 - Po uruchomieniu skanowania antywirusowego serwera, wykluczenia ze skanowania, dodane do iChecker, są resetowane po ponownym uruchomieniu serwera.
 - Technologia iSwift nie jest obsługiwany. Kaspersky Endpoint Security nie uwzględnia wykluczeń ze skanowania dodanych przy użyciu technologii iSwift.
 - Kaspersky Endpoint Security nie wykrywa plików eicar.com i susp-eicar.com, jeśli plik meicar.exe istniał na komputerze przed zainstalowaniem Kaspersky Endpoint Security.
 - Kaspersky Endpoint Security może niepoprawnie wyświetlać powiadomienia dotyczące leczenia zagrożeń. Na przykład, aplikacja może wyświetlić powiadomienie dotyczące zagrożenia dla wcześniej wyleczonego zagrożenia.
- Konfiguracje Server Core i Cluster Mode nie są obsługiwane.
- Technologie Szyfrowanie plików (FLE) i Kaspersky Disk Encryption (FDE) nie są obsługiwane na platformach serwerowych. Jednocześnie Kaspersky Endpoint Security może niepoprawnie przetwarzać zdarzenia dotyczące szyfrowania danych.
- Kontrola urządzeń nie jest obsługiwana na platformach serwerowych.
- W serwerowych systemach operacyjnych nie jest wyświetlane żadne ostrzeżenie dotyczące konieczności przeprowadzenia zaawansowanego leczenia.
- System Microsoft Windows Server 2008 został wykluczony ze wsparcia. - Instalowanie aplikacji na komputerze działającym pod kontrolą systemu operacyjnego Microsoft Windows Server 2008 nie jest obsługiwane.

[Obsługa platform wirtualnych](#)

- Szyfrowanie całego dysku (FDE) na maszynach wirtualnych Hyper-V nie jest obsługiwane.
- Szyfrowanie całego dysku (FDE) na platformach wirtualnych Citrix nie jest obsługiwane.
- Wielosesyjny Windows 10 Enterprise jest obsługiwany z ograniczeniami:
 - Kaspersky Endpoint Security uznaje wielosesyjny Windows 10 Enterprise jako serwerowy system operacyjny. Dlatego wielosesyjny Windows 10 Enterprise jest obsługiwany z ograniczeniami charakterystycznymi dla platform serwerowych. Na przykład, serwery nie mogą używać niektórych komponentów Kaspersky Endpoint Security. Aplikacja używa także klucza licencyjnego dla serwera zamiast klucza licencyjnego dla stacji roboczej.
 - Szyfrowanie całego dysku (FDE) nie jest obsługiwane.
 - Zarządzanie funkcją BitLocker nie jest obsługiwane.
 - Używanie Kaspersky Endpoint Security z dyskami wymiennymi nie jest obsługiwane. Infrastruktura Microsoft Azure definiuje dyski wymienne jako dyski sieciowe.
- Instalacja i używanie funkcji szyfrowania na poziomie plików (FLE) na platformach wirtualnych Citrix nie są obsługiwane.
- Aby włączyć kompatybilność Kaspersky Endpoint Security for Windows z Citrix PVS, wykonaj instalację z [włączoną opcją Zapewnij zgodność z Citrix PVS](#). Ta opcja może być włączona w [Kreatorze instalacji](#) lub przy użyciu [parametru wiersza poleceń](#) /pCITRIXCOMPATIBILITY=1. W przypadku zdalnej instalacji należy zmodyfikować [plik KUD](#), dodając do niego następujący parametr: /pCITRIXCOMPATIBILITY=1.
- Citrix XenDesktop. Przed rozpoczęciem klonowania należy [wyłączyć autoochronę](#), aby klonować maszyny wirtualne, które korzystają z vDisk.
- Przygotowując urządzenie szablonowe do głównego obrazu Citrix XenDesktop z zainstalowanym programem Kaspersky Endpoint Security for Windows i Agentem sieciowym Kaspersky Security Center, dodaj do pliku konfiguracyjnego następujące typy wykluczeń:


```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky\**\*"
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

Więcej informacji o Citrix XenDesktop można znaleźć na [stronie internetowej pomocy technicznej Citrix](#).
- W niektórych przypadkach próba bezpiecznego odłączenia nośnika wymiennego może zakończyć się niepowodzeniem na maszynie wirtualnej, która jest wdrażana na hipernadzorcy VMware ESXi. Spróbuj ponownie bezpiecznie odłączyć urządzenie.

[Kompatybilność z Kaspersky Security Center](#)

- Możesz zarządzać komponentem Adaptacyjna kontrola anomalii tylko w Kaspersky Security Center w wersji 11 lub nowszej.
- Raport Kaspersky Security Center 11 dotyczący zagrożeń może nie zawierać informacji dotyczących działania podejmowanego na zagrożeniach, które zostały wykryte przez komponent Ochrona AMSI.
- Stan działania komponentów Ochrona AMSI i Adaptacyjna kontrola anomalii jest dostępna tylko w Kaspersky Security Center w wersji 11 lub nowszej. Możesz przejrzeć stan działania w Kaspersky Security Center Console w obrębie właściwości komputera, w sekcji **Zadania**. Raporty dotyczące tych komponentów są także dostępne tylko w Kaspersky Security Center w wersji 11 lub nowszej.

Licencjonowanie

- Jeśli zostanie wyświetlona wiadomość systemowa *Błąd podczas pobierania danych*, sprawdź, czy komputer, na którym przeprowadzasz aktywację, posiada dostęp do sieci, bądź też skonfiguruj ustawienia aktywacji poprzez Kaspersky Security Center Activation Proxy.
- Aplikacja nie może zostać aktywowana przez subskrypcję za pośrednictwem Kaspersky Security Center, jeśli licencja utraciła ważność lub jeśli licencja testowa jest aktywna na komputerze. Aby zastąpić licencję testową lub licencję, która wkrótce utraci ważność, licencją subskrypcyjną, [użyj zadania dystrybucji licencji](#).
- W interfejsie aplikacji data wygaśnięcia licencji jest wyświetlana w czasie lokalnym komputera.
- Instalacja aplikacji z osadzonym plikiem klucza na komputerze, który posiada niestabilny dostęp do internetu, może powodować tymczasowe wyświetlanie zdarzeń informujących, że aplikacja nie została aktywowana lub licencja nie pozwala na działanie komponentu. Jest to spowodowane tym, że aplikacja w pierwszej kolejności przeprowadza instalację, a następnie aktywację osadzonej licencji testowej, co wymaga dostępu do internetu w celu zapewnienia aktywacji podczas procedury instalacji.
- W trakcie obowiązywania okresu testowego instalacja dowolnej aktualizacji lub łaty aplikacji na komputerze, na którym jest niestabilne połączenie z internetem, może wpływać na tymczasowe wyświetlanie zdarzeń informujących, że aplikacja nie została aktywowana. Jest to spowodowane tym, że aplikacja w pierwszej kolejności przeprowadza instalację, a następnie aktywację osadzonej licencji testowej, co wymaga dostępu do internetu w celu zapewnienia aktywacji podczas instalacji lub aktualizacji.
- Jeśli licencja testowa została automatycznie aktywowana podczas instalacji aplikacji, a następnie aplikacja została usunięta bez zapisywania informacji o licencji, aplikacja nie zostanie automatycznie aktywowana z licencją testową po ponownej instalacji. W tym przypadku przeprowadź ręczną aktywację aplikacji.
- Jeśli korzystasz z Kaspersky Security Center w wersji 11 oraz w Kaspersky Endpoint Security w wersji 11.7.0, raporty z działania komponentu mogą nie działać poprawnie. Jeśli zainstalowałeś komponenty Kaspersky Endpoint Security, które nie znajdują się w Twojej licencji, Agent sieciowy może wysłać błędy o stanie komponentów do dziennika zdarzeń systemu Windows. Aby uniknąć błędów, usuń komponenty, które nie znajdują się w Twojej licencji.

Silnik korygujący

- Aplikacja przywraca pliki tylko na urządzeniach, które posiadają system plików NTFS lub FAT32.
- Aplikacja przywraca pliki z następującymi rozszerzeniami: odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsx, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd.
- Nie jest możliwe przywrócenie plików przechowywanych na dyskach sieciowych lub na dyskach CD/DVD wielokrotnego zapisu.
- Nie jest możliwe przywrócenie plików, które zostały zaszyfrowane za pomocą systemu szyfrowania plików (EFS). Więcej informacji na temat działania EFS znajdziesz na [stronie internetowej firmy Microsoft](#).
- Aplikacja nie monitoruje modyfikacji na plikach, wykonywanych przez procesy na poziomie jądra systemu operacyjnego.
- Aplikacja nie monitoruje modyfikacji wykonywanych na plikach z poziomu interfejsu sieciowego (na przykład, jeśli plik jest przechowywany w folderze współdzielonym, a proces jest uruchamiany zdalnie z poziomu innego komputera).

[Zapora sieciowa](#)

- Filtrowanie pakietów lub połączeń według adresu lokalnego, interfejsu fizycznego i czasu życia pakietu (TTL) jest obsługiwane w następujących przypadkach:
 - Według adresu lokalnego dla pakietów lub połączeń wychodzących w regułach dla aplikacji (dla portu TCP i UDP) i regułach dla pakietów.
 - Według adresu lokalnego dla pakietów lub połączeń przychodzących (za wyjątkiem portu UDP) w regułach blokowania aplikacji i regułach dla pakietów.
 - Według czasu życia pakietu (TTL) w regułach blokowania dla pakietów przychodzących lub wychodzących.
 - Według interfejsu sieciowego dla pakietów lub połączeń przychodzących i wychodzących w regułach dla pakietów.
- W wersjach 11.0.0 i 11.0.1 zdefiniowane adresy MAC są niepoprawnie zastosowane. Ustawienia adresu MAC dla wersji 11.0.0, 11.0.1 i 11.1.0 lub nowszej nie są kompatybilne. Po zaktualizowaniu aplikacji lub wtyczki z tych wersji do wersji 11.1.0 lub nowszej, musisz zweryfikować i ponownie skonfigurować zdefiniowane adresy MAC w regułach Zapory sieciowej.
- Podczas aktualizacji aplikacji z wersji 11.1.1 i 11.2.0 do wersji 11.7.0 stany uprawnień dla następujących reguł Zapory sieciowej nie zostały przeniesione:
 - Żądania wysyłane do serwera DNS po protokole TCP.
 - Żądania wysyłane do serwera DNS po protokole UDP.
 - Dowolna aktywność sieciowa.
 - Odpowiedzi przychodzące protokołu ICMP typu „Cel nieosiągalny”.
 - Przychodzący strumień ICMP.
- Jeśli skonfigurowałeś kartę sieciową lub czas wygaśnięcia pakietu (TTL) dla zezwalającej reguły dla pakietu, priorytet tej reguły jest mniejszy niż blokująca reguła dla aplikacji. Innymi słowy, jeśli aktywność sieciowa jest zablokowana dla aplikacji (na przykład, aplikacja jest w grupie zaufania *Wysoki poziom ograniczeń*), nie można zezwolić na aktywność sieciową aplikacji przy użyciu reguły dla pakietu z tymi ustawieniami. We wszystkich pozostałych przypadkach priorytet reguły dla pakietu jest wyższy niż reguła sieciowa dla aplikacji.
- Podczas [importowania reguł dla pakietów Zapory sieciowej](#) program Kaspersky Endpoint Security może modyfikować nazwy reguł. Aplikacja określa reguły z identycznymi zestawami parametrów ogólnych: protokół, kierunek, porty zdalne i lokalne, czas wygaśnięcia pakietu (TTL). Jeśli ten zestaw parametrów ogólnych jest identyczny dla kilku reguł, aplikacja przypisze tę samą nazwę do tych reguł lub doda znacznik parametru do nazwy. W ten sposób Kaspersky Endpoint Security importuje wszystkie reguły dla pakietów, ale nazwa reguł, które posiadają identyczne ustawienia ogólne, może zostać zmodyfikowana.
- Jeśli [w regule sieciowej włączyłeś raportowanie o zdarzeniach aplikacji](#), podczas przenoszenia aplikacji do innej grupy zaufania ograniczenia tejże grupy nie będą stosowane. Dlatego, jeśli aplikacja znajduje się w grupie Zaufane, nie będzie posiadała żadnych ograniczeń sieciowych. Następnie włączyłeś raportowanie o zdarzeniach dla tej aplikacji i przeniósłeś ją do grupy Niezaufane. Zapora sieciowa nie wymusi ograniczeń sieciowych dla tej aplikacji. Zalecane jest, abyś w pierwszej kolejności przeniósł aplikację do odpowiedniej grupy zaufania, a następnie włączył raportowanie o zdarzeniach. Jeśli ta metoda nie jest odpowiednia, możesz ręcznie skonfigurować ograniczenia dla aplikacji w ustawieniach reguły sieciowej. Ograniczenie jest stosowane tylko do lokalnego interfejsu aplikacji. Przenoszenie aplikacji między grupami zaufania w zasadzie działa poprawnie.

- Komponenty Zapora sieciowa i Ochrona przed włamaniami posiadają wspólne ustawienia: uprawnienia aplikacji i chronione zasoby. Jeśli zmienisz te ustawienia dla Zapory sieciowej, Kaspersky Endpoint Security automatycznie zastosuje nowe ustawienia do Ochrony przed włamaniami. Jeśli, na przykład, zezwoliłeś na zmiany w ustawieniach głównej zasady Zapory sieciowej (kłódka jest otwarta), ustawienia Ochrony przed włamaniami także staną się dostępne do edycji.
- Jeśli reguła dla pakietu sieciowego została wyzwolona w Kaspersky Endpoint Security 11.6.0 lub wcześniejszej wersji, kolumna **Nazwa aplikacji** w raporcie Zapory sieciowej będzie zawsze wyświetlała wartość *Kaspersky Endpoint Security*. Dodatkowo, Zapora sieciowa zablokuje połączenie na poziomie pakietów dla wszystkich aplikacji. To zachowanie zostało zmodyfikowane dla Kaspersky Endpoint Security 11.7.0 lub nowszej wersji. Kolumna **Typ reguły** została dodana do raportu Zapory sieciowej. Jeśli reguła dla pakietu sieciowego zostanie wyzwolona, wartość w kolumnie **Nazwa aplikacji** pozostanie pusta.

Ochrona przed atakami BadUSB

- Kaspersky Endpoint Security resetuje limit czasu blokady urządzenia USB, gdy komputer jest zablokowany (na przykład, minął limit czasu blokady ekranu). Oznacza to, że jeśli kilka razy wprowadzono zły kod autoryzacyjny dla urządzenia USB i aplikacja zablokuje urządzenie USB, Kaspersky Endpoint Security zezwoli na powtórzenie próby autoryzacji po odblokowaniu komputera. W tym przypadku Kaspersky Endpoint Security nie zablokuje urządzenia USB na czas określony w [ustawieniach komponentu Ochrona przed atakami BadUSB](#).
- Kaspersky Endpoint Security resetuje limit czasu blokady urządzenia USB, gdy [ochrona komputera jest wstrzymana](#). Oznacza to, że jeśli kilka razy wprowadzono zły kod autoryzacyjny dla urządzenia USB i aplikacja zablokuje urządzenie USB, Kaspersky Endpoint Security zezwoli na powtórzenie próby autoryzacji po [wznowieniu ochrony komputera](#). W tym przypadku Kaspersky Endpoint Security nie zablokuje urządzenia USB na czas określony w [ustawieniach komponentu Ochrona przed atakami BadUSB](#).

Kontrola aplikacji

- Podczas pracy w systemie Microsoft Windows 10 trybie listy zablokowanych aplikacji, blokowanie reguł może być niepoprawnie zastosowane, co może spowodować blokowanie aplikacji, które nie zostały określone w regułach.
- Jeśli progresywne aplikacje internetowe (PWA) są blokowane przez komponent Kontrola aplikacji, plik appManifest.xml został wskazany jako zablokowana aplikacja w raporcie.
- Podczas dodawania standardowej aplikacji Notatnik do reguły Kontroli aplikacji dla systemu Windows 11, nie jest zalecane określenie ścieżki do aplikacji. Na komputerach działających pod kontrolą systemu Windows 11, system operacyjny używa aplikacji Notatnik Metro, znajdującej się w folderze C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe. W poprzednich wersjach systemu operacyjnego, Notatnik znajduje się w następujących folderach:
 - C:\Windows\notepad.exe
 - C:\Windows\System32\notepad.exe
 - C:\Windows\SysWOW64\notepad.exe

Podczas dodawania Notatnika do reguły Kontroli aplikacji, możesz określić nazwę aplikacji i sumę kontrolną pliku z właściwości uruchomionej aplikacji.

Kontrola urządzeń

- Dostęp do Drukarek dodanych do listy zaufanych urządzeń jest blokowany przez reguły blokowania magistral i urządzeń.
- Dla urządzeń MTP kontrola działań Odczyt, Zapis i Podłącz jest obsługiwana, jeśli korzystasz z wbudowanego sterownika Microsoft systemu operacyjnego. Jeśli użytkownik instaluje niestandardowy sterownik do pracy z urządzeniem (na przykład, jako część iTunes lub Android Debug Bridge), kontrola działań Odczyt i Zapis może nie działać.
- Podczas pracy z urządzeniami MTP, reguły dostępu zostaną zmienione po ponownym podłączeniu urządzenia.
- Jeśli dodasz urządzenie do listy zaufanych w oparciu o maskę modelu i używane znaki, które znajdują się w identyfikatorze, a nie w nazwie modelu, te urządzenia nie zostaną dodane. Na stacji roboczej te urządzenia zostaną dodane do listy zaufanych w oparciu o maskę identyfikatora.

Kontrola sieci

- Formaty OGV i WEBM nie są obsługiwane.
- Protokół RTMP nie jest obsługiwany.

Adaptacyjna kontrola anomalii

- Zalecane jest automatyczne utworzenie wykluczeń w oparciu o zdarzenie. Jeśli ręcznie dodajesz wykluczenie, podczas obiektu docelowego, do początku ścieżki dodaj znak `*`.
- Raport reguły Adaptacyjnej kontroli anomalii nie może zostać wygenerowany, jeśli próbka zawiera chociaż jedno zdarzenie, którego nazwa zawiera ponad 260 znaków.
- Dodawanie wykluczeń z repozytorium Wywoływanie reguł Adaptacyjnej kontroli anomalii nie jest obsługiwane, jeśli właściwości obiektu lub procesu posiadają wartość zawierającą ponad 256 znaków (na przykład, ścieżka do obiektu docelowego). Możesz ręcznie dodać wykluczenie w ustawieniach zasady. Możesz także dodać wykluczenie w Raporcie dotyczącym wyzwolonych reguł Adaptacyjnej kontroli anomalii.

Szyfrowanie dysku (FDE)

- Po zainstalowaniu aplikacji, w celu zapewnienia poprawnego działania należy ponownie uruchomić system operacyjny dla szyfrowania dysku twardego.
- Agent autoryzacji nie obsługuje hieroglifów i znaków specjalnych ¶ i \.
- W celu zapewnienia optymalnego działania komputera po szyfrowaniu, wymagane jest, aby procesor obsługiwał zestaw instrukcji AES-NI (Intel Advanced Encryption Standard New Instructions). Jeśli procesor nie obsługuje AES-NI, wydajność komputera może spadać.
- Jeśli istnieją procesy próbujące uzyskać dostęp do zaszyfrowanych urządzeń zanim aplikacja udzieliła dostępu do tych urządzeń, aplikacja wyświetli ostrzeżenie dotyczące zakończenia działania tych procesów. Jeśli procesy nie mogą zostać zakończone, ponownie podłącz zaszyfrowane urządzenia.
- Unikatowy numer ID dysków twardech jest wyświetlany w statystykach szyfrowania urządzeń, w formacie odwróconym.
- Podczas szyfrowania urządzeń nie jest zalecane ich formatowanie.
- Jeśli kilka nośników wymiennych jest podłączonych do komputera w tym samym czasie, zasada szyfrowania może zostać zastosowana tylko do jednego nośnika wymiennego. Jeśli nośniki wymienne zostaną podłączone ponownie, zasada szyfrowania została zastosowana poprawnie.
- Proces szyfrowania może nie rozpocząć się na mocno pofragmentowanym dysku twardym. Zdefragmentuj dysk twardy.
- Podczas szyfrowania dysków twardech, hibernacja jest blokowana od momentu rozpoczęcia zadania szyfrowania, aż do pierwszego ponownego uruchomienia komputera z systemem operacyjnym Microsoft Windows 7/8/8.1/10, a w przypadku zainstalowania szyfrowania dysku twardego, aż do pierwszego ponownego uruchomienia systemu operacyjnego Microsoft Windows 8/8.1/10. W przypadku deszyfrowania dysku twardego hibernacja jest blokowana od momentu całkowitego odszyfrowania sektorów startowych dysku twardego, aż do pierwszego ponownego uruchomienia systemu operacyjnego. Jeśli w systemie operacyjnym Microsoft Windows 8/8.1/10 włączona jest opcja **Szybki start**, zablokowanie hibernacji uniemożliwia zamknięcie systemu operacyjnego.
- Komputery z systemem Windows 7 nie pozwalają na zmianę hasła podczas wykrywania szyfrowania dysku przy użyciu technologii BitLocker. Po wprowadzeniu klucza odzyskiwania i załadowaniu systemu operacyjnego, program Kaspersky Endpoint Security nie wyświetli monitu o zmianę hasła lub kodu PIN. Dlatego też niemożliwe jest ustawienie nowego hasła lub kodu PIN. Ten problem jest spowodowany przez szczególne właściwości systemu operacyjnego. Aby kontynuować, należy ponownie zaszyfrować dysk twardy.
- Nie jest zalecane użycie narzędzia xbootmgr.exe z włączonymi dodatkowymi opcjami. Na przykład: Dispatcher, Network lub Drivers.
- Formatowanie zaszyfrowanego nośnika wymiennego nie jest obsługiwane na komputerze z zainstalowanym programem Kaspersky Endpoint Security for Windows.
- Formatowanie zaszyfrowanego nośnika wymiennego z systemem plików FAT32 nie jest obsługiwane (dysk jest wyświetlany jako zaszyfrowany). W celu sformatowania dysku, ponownie sformatuj go do system plików NTFS.
- Więcej informacji na temat przywracania systemu operacyjnego z kopii zapasowej do zaszyfrowanego urządzenia GPT zostały opisane [na stronie Bazy wiedzy pomocy technicznej](#).
- Na jednym zaszyfrowanym komputerze nie może istnieć kilku agentów pobierania.

- Nie można uzyskać dostępu do nośnika wymiennego, który wcześniej został zaszyfrowany na innym komputerze, jeśli jednocześnie spełnione są wszystkie z następujących warunków:

- Brak połączenia z serwerem Kaspersky Security Center.
- Użytkownik podejmuje próbę uwierzytelnienia przy użyciu nowego tokena lub hasła.

Jeśli wystąpi podobna sytuacja, uruchom komputer ponownie. Po ponownym uruchomieniu komputera, dostęp do zaszyfrowanego nośnika wymiennego zostanie udzielony.

- Wykrycie urządzeń USB przez Agenta autoryzacji może nie być obsługiwane, jeśli w ustawieniach BIOS-u, dla USB włączony jest tryb xHCI.
- Kaspersky Disk Encryption (FDE) dla dysku SSD, który jest używany do buforowania najczęściej używanych danych, nie jest obsługiwane dla urządzeń SSHD.
- Szyfrowanie dysków twardych w 32-bitowych systemów operacyjnych Microsoft Windows 8/8.1/10, działających w trybie UEFI, nie jest obsługiwane.
- Uruchom komputer ponownie przed ponownym zaszyfrowaniem odszyfrowanego dysku twardego.
- Szyfrowanie dysku twardego nie jest kompatybilne z Kaspersky Anti-Virus dla UEFI. Nie jest zalecane używanie funkcji szyfrowania dysku twardego na komputerach, na których jest zainstalowany Kaspersky Anti-Virus dla UEFI.
- [Tworzenie kont Agenta autoryzacji](#) w oparciu o konta Microsoft jest obsługiwane z następującymi ograniczeniami:
 - Nie jest obsługiwana technologia [logowania jednokrotnego](#).
 - Automatyczne tworzenie kont Agenta autoryzacji nie jest obsługiwane, jeśli została wybrana opcja tworzenia kont dla użytkowników, którzy logowali się do systemu w ciągu ostatnich N dni.
- Jeśli nazwa konta Agenta autoryzacji posiada format <domena>/<nazwa konta Windows>, po zmianie nazwy komputera, musisz także zmienić nazwy kont, które zostały utworzone dla lokalnych użytkowników tego komputera. Na przykład, wyobraź sobie, że na komputerze Ivanov istnieje lokalny użytkownik Ivanov, a dla tego użytkownika utworzono konto Agenta autoryzacji o nazwie Ivanov/Ivanov. Jeśli nazwa komputera Ivanov została zmieniona na Ivanov-PC, musisz zmienić nazwę konta Agenta autoryzacji dla użytkownika Ivanov z Ivanov/Ivanov na Ivanov-PC/Ivanov. Możesz zmienić nazwę konta przy użyciu zadania zarządzania kontem lokalnym Agenta autoryzacji. Przed zmianą nazwy konta, uwierzytelnianie w środowisku wykonawczym przed uruchomieniem systemu jest możliwe przy użyciu starej nazwy (na przykład: Ivanov/Ivanov).
- Jeśli użytkownik może uzyskać dostęp do komputera, który został zaszyfrowany z użyciem technologii Kaspersky Disk Encryption tylko przy użyciu tokena, a ten użytkownik musi zakończyć procedurę odzyskiwania dostępu, upewnij się, że po przywróceniu dostępu do zaszyfrowanego komputera temu użytkownikowi można udzielić dostępu z użyciem hasła do tego komputera. Hasło, które użytkownik ustawił podczas przywracania dostępu, może nie zostać zapisane. W tym przypadku użytkownik będzie musiał ponownie zakończyć procedurę przywracania dostępu do zaszyfrowanego komputera przy jego kolejnym ponownym uruchomieniu.
- Podczas odszyfrowywania dysku twardego przy użyciu narzędzia [FDE Recovery Tool](#), proces deszyfracji może zakończyć się błędem, jeśli dane na urządzeniu źródłowym zostaną nadpisane odszyfrowanymi danymi. Część danych na dysku twardym pozostanie zaszyfrowana. Zalecane jest wybranie opcji zapisu odszyfrowanych danych do pliku w ustawieniach odszyfrowywania urządzenia podczas korzystania z FDE Recovery Tool.

- Jeśli hasło do Agenta autoryzacji zostało zmienione, zostanie wyświetlona wiadomość *Twoje hasło zostało pomyślnie zmienione. Kliknij OK*, a użytkownik uruchomi komputer ponownie, nowe hasło nie zostanie zapisane. Stare hasło musi być używane do kolejnego uwierzytelniania w środowisku wykonawczym przed uruchomieniem systemu.
- Szyfrowanie dysku jest niekompatybilne z technologią Intel Rapid Start.
- Szyfrowanie dysku jest niekompatybilne z technologią ExpressCache.
- W niektórych przypadkach, podczas próby odszyfrowania zaszyfrowanego dysku przy użyciu [FDE Recovery Tool](#), po zakończeniu procedury „Żądanie-Odpowiedź” narzędzie błędnie wykrywa stan urządzenia jako „niezaszyfrowane”. Raport narzędzia wyświetla zdarzenie informujące, że urządzenie zostało pomyślnie odszyfrowane. W tym przypadku należy ponownie uruchomić procedurę odzyskiwania danych, aby odszyfrować urządzenie.
- Po zaktualizowaniu wtyczki Kaspersky Endpoint Security for Windows w konsoli Web Console, właściwości komputera klienckiego nie wyświetlają klucza odzyskiwania BitLocker, aż usługa Web Console nie zostanie ponownie uruchomiona.
- Aby zobaczyć inne ograniczenia obsługi szyfrowania całego dysku oraz listę urządzeń, dla których szyfrowanie dysków twardych jest obsługiwane z ograniczeniami, zapoznaj się z [Bazą wiedzy, dostępną na stronie pomocy technicznej](#) .

[Szyfrowanie plików \(FLE\)](#)

- Szyfrowanie plików i folderów nie jest obsługiwane w systemach operacyjnych z rodziny Microsoft Windows Embedded.
- Po zainstalowaniu aplikacji, musisz ponownie uruchomić system operacyjny, aby szyfrowanie plików i folderów działało poprawnie.
- Jeśli zaszyfrowany plik jest przechowywany na komputerze, który posiada dostępną funkcję szyfrowania, a użytkownik uzyskuje dostęp do pliku z komputera, na którym szyfrowanie nie jest dostępne, bezpośredni dostęp do tego pliku zostanie udzielony. Zaszyfrowany plik przechowywany w folderze sieciowym na komputerze, na którym jest dostępna funkcjonalność szyfrowania, zostanie skopiowany w postaci odszyfrowanej na komputer, na którym nie ma dostępnej funkcjonalności szyfrowania.
- Przed zaszyfrowaniem plików przy użyciu Kaspersky Endpoint Security for Windows zalecane jest odszyfrowanie plików, które zostały zaszyfrowane za pomocą systemu szyfrowania plików EFS.
- Po zaszyfrowaniu pliku, jego rozmiar zwiększy się o 4 kB.
- Po zaszyfrowaniu pliku, w jego właściwościach zostanie ustawiony atrybut *Archiwum*.
- Jeśli nierozpakowany plik z zaszyfrowanego archiwum posiada taką samą nazwę co już istniejący plik na komputerze, ten istniejący zostanie nadpisany przez nowy plik, który został wypakowany z zaszyfrowanego archiwum. Użytkownik nie zostaje poinformowany o działaniu nadpisania.
- Przed wyodrębnieniem zaszyfrowanego archiwum należy upewnić się, że jest wystarczająco dużo wolnego miejsca na dysku, aby pomieścić wyodrębnione pliki. Jeśli nie ma wystarczającej ilości miejsca na dysku, wyodrębnianie archiwum może zostać ukończone, ale pliki mogą być uszkodzone. W takim przypadku możliwe jest, że Kaspersky Endpoint Security nie wyświetli żadnych komunikatów o błędach.
- Interfejs [Przenośnego Menedżera plików](#) nie wyświetla wiadomości o błędach, które występują podczas jego działania.
- Kaspersky Endpoint Security for Windows nie uruchamia [Przenośnego Menedżera plików](#) na komputerze, na którym jest zainstalowany komponent Szyfrowanie plików.
- Nie możesz użyć [Przenośnego menedżera plików](#) do uzyskania dostępu do dysku wymiennego, jeśli następujące warunki są spełnione jednocześnie:
 - Brak połączenia z Kaspersky Security Center;
 - Kaspersky Endpoint Security for Windows jest zainstalowany na komputerze;
 - Szyfrowanie danych (FDE lub FLE) nie zostało wykonane na komputerze.

Dostęp nie jest możliwy nawet wtedy, gdy znasz hasło do Przenośnego menedżera plików.

- Jeśli używana jest funkcja szyfrowania plików, aplikacja jest niekompatybilna z klientem pocztowym Sylpheed.
- Kaspersky Endpoint Security for Windows nie obsługuje [reguł ograniczeń dostępu do zaszyfrowanych plików](#) dla niektórych aplikacji. Wynika to z faktu, że niektóre operacje na plikach są wykonywane przez inne aplikacje. Na przykład, kopiowanie plików jest wykonywane przez menedżera plików, a nie przez samą aplikację. W ten sposób, jeżeli klientowi poczty Outlook odmówiono dostępu do zaszyfrowanych plików, Kaspersky Endpoint Security pozwoli klientowi poczty na dostęp do zaszyfrowanego pliku, jeżeli użytkownik skopiował pliki do wiadomości e-mail za pomocą schowka lub używając funkcji „przeciągnij i upuść”. Czynność kopiowania została wykonana przez menedżera plików, dla którego nie zostały określone zasady ograniczania dostępu do zaszyfrowanych plików, tzn. dostęp jest dozwolony.

- Jeśli nośniki wymienne są zaszyfrowane z [obsługą trybu przenośnego](#), kontrola ważności hasła nie może zostać wyłączona.
- Zmiana ustawień plików stronicowania nie jest obsługiwana. System operacyjny używa domyślnych wartości zamiast określonych wartości parametrów.
- Podczas pracy z zaszyfrowanymi nośnikami wymiennymi należy użyć bezpiecznego usuwania. Nie można zagwarantować integralności danych, jeśli nośnik wymienny nie został bezpiecznie usunięty.
- Po zaszyfrowaniu plików ich oryginalne niezasyfrowane kopie są bezpiecznie usuwane.
- Synchronizacja plików offline przy użyciu usługi Buforowanie po stronie klienta (CSC) nie jest obsługiwana. Zalecane jest zablokowanie zarządzania offline współdzielonymi zasobami na poziomie zasady grupy. Pliki, które są w trybie offline, mogą być edytowane. Po synchronizacji, zmiany wprowadzone w pliku offline mogą zostać utracone. Więcej informacji dotyczących obsługi Buforowania po stronie klienta (CSC) podczas korzystania z szyfrowania można znaleźć w [Bazie wiedzy na stronie pomocy technicznej](#).
- [Tworzenie zaszyfrowanego archiwum](#) na głównym dysku twardym nie jest obsługiwane.
- Podczas uzyskiwania dostępu do zaszyfrowanych plików poprzez sieć mogą pojawić się problemy. Zalecane jest przeniesienie plików do innego źródła lub upewnienie się, że komputer używany jako serwer plików jest zarządzany przez ten sam Serwer administracyjny Kaspersky Security Center.
- Zmiana układu klawiatury powoduje brak odpowiedzi okna do wprowadzenia hasła do zaszyfrowanego samorozpakowującego się archiwum. Aby rozwiązać ten problem, zamknij okno do wprowadzenia hasła, przełącz układ klawiatury w swoim systemie operacyjnym, a następnie ponownie wprowadź hasło do zaszyfrowanego archiwum.
- Jeśli szyfrowanie plików jest używane na systemach, które posiadają kilka partycji na jednym dysku, zalecane jest użycie opcji, która automatycznie określa rozmiar pliku pagefile.sys. Po ponownym uruchomieniu komputera plik pagefile.sys może zostać przenoszony między partycjami dysku.
- Po zastosowaniu reguł szyfrowania plików, w tym plików w folderze Moje dokumenty, upewnij się, że użytkownicy, dla których szyfrowanie zostało zastosowane, mogą pomyślnie uzyskać dostęp do zaszyfrowanych plików. Aby to zrobić, każdy użytkownik loguje się do systemu, w którym dostępne jest połączenie z Kaspersky Security Center. Jeśli użytkownik spróbuje uzyskać dostęp do zaszyfrowanych plików bez połączenia z Kaspersky Security Center, system może się zawieszać.
- Jeśli pliki systemowe są w jakiś sposób uwzględnione w obszarze szyfrowania plików, w raportach mogą pojawić się zdarzenia dotyczące błędów, które wystąpiły podczas szyfrowania tych plików. Pliki określone w tych zdarzeniach nie są tak naprawdę szyfrowane.
- Procesy Pico nie są obsługiwane.
- Ścieżki uwzględniające wielkość liter nie są obsługiwane. Jeśli reguły szyfrowania lub reguły deszyfrowania zostaną zastosowane, ścieżki w zdarzeniach produktu są napisane małymi literami.
- Nie jest zalecane szyfrowanie plików, które są używane przez system podczas uruchamiania. Jeśli te pliki są zaszyfrowane, próba dostępu do zaszyfrowanych plików bez połączenia z Kaspersky Security Center może powodować zawieszanie się systemu lub doprowadzić do wyświetlenia monitów o dostęp do odszyfrowanych plików.
- Jeśli użytkownicy wspólnie pracują z plikiem poprzez sieć zgodnie z regułami FLE za pośrednictwem aplikacji, które wykorzystują metodę mapowania wczytywania pliku do pamięci (np. WordPad lub FAR) oraz aplikacje zaprojektowane do pracy z dużymi plikami (np. Notepad ++), plik w postaci zaszyfrowanej może zostać zablokowany niezależnie bez możliwości uzyskania dostępu do niego z poziomu komputera, na którym się znajduje.

- Szyfrowanie plików w folderach synchronizacji OneDrive nie jest obsługiwane. Dodawanie folderów z już zaszyfrowanymi plikami do listy synchronizacji OneDrive może powodować utratę danych w plikach zaszyfrowanych.
- Jeśli zainstalowano komponent szyfrowania plików, zarządzanie użytkownikami i grupami nie działa w trybie WSL (podsystem Windows dla systemu Linux).
- Po zainstalowaniu komponentu szyfrowania plików, tryb POSIX (Portable Operating System Interface) do zmiany nazwy i usuwania plików nie jest obsługiwany.
- Nie zaleca się szyfrowania plików tymczasowych, ponieważ może to spowodować utratę danych. Na przykład Microsoft Word tworzy pliki tymczasowe podczas przetwarzania dokumentu. Jeśli pliki tymczasowe zostaną zaszyfrowane, ale oryginalny plik nie, podczas próby zapisania dokumentu może wystąpić błąd *Odmowa dostępu*. Dodatkowo Microsoft Word może zapisać plik, ale nie będzie można otworzyć dokumentu następnym razem, czyli dane zostaną utracone. Aby zapobiec utracie danych, należy [wykluczyć folder plików tymczasowych z reguł szyfrowania](#).
- Po aktualizacji Kaspersky Endpoint Security for Windows w wersji 11.0.1 lub wcześniejszej, aby uzyskać dostęp do zaszyfrowanych plików po ponownym uruchomieniu komputera, upewnij się, że Agent sieciowy jest uruchomiony. Agent sieciowy ma opóźniony start, więc nie można uzyskać dostępu do zaszyfrowanych plików natychmiast po załadowaniu systemu operacyjnego. Nie trzeba czekać na uruchomienie Agenta sieciowego po kolejnym uruchomieniu komputera.

[Inne ograniczenia](#)

- Adresy internetowe, które są [dodawane do listy zaufanych](#), mogą zostać niepoprawnie przetworzone.
- Kontrola systemu. Wszystkie informacje o procesach nie są wyświetlane.
- Jeśli Kaspersky Endpoint Security for Windows jest uruchamiany po raz pierwszy, aplikacja z podpisem cyfrowym może być tymczasowo umieszczona w złej grupie. Aplikacja z podpisem cyfrowym zostanie później umieszczona we właściwej grupie.
- Podczas skanowania poczty z użyciem [rozszerzenia modułu Ochrona poczty dla Microsoft Outlook](#) zalecane jest korzystanie z trybu buforowanego programu Exchange (opcja Użyj trybu buforowanej wymiany).
- [Zadanie Skanowanie antywirusowe](#) nie obsługuje 64-bitowej wersji systemu Microsoft Outlook. To oznacza, że Kaspersky Endpoint Security nie sprawdza plików Outlook x64 (pliki PST i OST) nawet wtedy, gdy [poczta zostaje uwzględniona w obszarze skanowania](#).
- W Kaspersky Security Center 10, podczas przełączania z korzystania z globalnej sieci Kaspersky Security Network na korzystanie z prywatnej sieci Kaspersky Security Network lub vice versa, [opcja uczestniczenia w Kaspersky Security Network jest wyłączona](#) w zasadzie określonego produktu. Po przełączeniu uważnie przeczytaj treść Oświadczenia Kaspersky Security Network i potwierdź chęć uczestnictwa w KSN. Możesz przeczytać treść Oświadczenia w interfejsie aplikacji lub podczas edytowania zasady produktu.
- Podczas ponownego skanowania szkodliwego obiektu, który został zablokowany przez oprogramowanie innej firmy, użytkownik nie zostanie poinformowany po ponownym wykryciu zagrożenia. Zdarzenie dotyczące ponownego wykrycia zagrożenia zostanie wyświetlone jako zdarzenie w raporcie produktu i w raporcie Kaspersky Security Center 10.
- Komponent [Endpoint Sensor](#) nie może zostać zainstalowany w Microsoft Windows Server 2008.
- Raport z szyfrowania urządzenia w Kaspersky Security Center 10 nie będzie zawierał informacji o urządzeniach, które zostały zaszyfrowane przy użyciu technologii Microsoft BitLocker na platformach serwerowych lub na stacjach roboczych, na których nie zainstalowano komponentu Kontrola urządzeń.
- Nie można włączyć wyświetlania wszystkich wpisów w raporcie w konsoli Kaspersky Security Center Web Console. W konsoli Web Console możesz zmienić tylko liczbę wpisów wyświetlanych w raportach. Domyślnie, Kaspersky Security Center Web Console wyświetla 1000 wpisów w raporcie. Możesz włączyć wyświetlanie wszystkich wpisów w raporcie w Konsoli administracyjnej (MMC).
- Nie można ustawić wyświetlania więcej niż 1000 wpisów w raporcie w konsoli Kaspersky Security Center Console. Jeśli ustawisz wartość wyższą niż 1000, konsola Kaspersky Security Center Console wyświetli tylko 1000 wpisów w raporcie.
- Podczas korzystania z hierarchii zasad ustawienia sekcji Szyfrowanie nośników wymiennych w zasadzie potomnej są dostępne do edycji, jeśli zasada nadrzędna zapobiega modyfikacji tych ustawień.
- Musisz włączyć Przeprowadź inspekcję logowania w ustawieniach systemu operacyjnego, aby zapewnić poprawne funkcjonowanie [wykluczeń dla ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem](#).
- Jeśli [ochrona folderu współdzielonego jest wyłączona](#), Kaspersky Endpoint Security for Windows monitoruje próby szyfrowania folderów współdzielonych dla każdej sesji zdalnego dostępu, które zostało uruchomione przed uruchomieniem Kaspersky Endpoint Security for Windows, w tym, jeśli komputer, z którego sesja zdalnego dostępu została uruchomiona, została dodana do wykluczeń. Jeśli nie chcesz, żeby Kaspersky Endpoint Security for Windows monitorował próby szyfrowania folderów współdzielonych dla sesji zdalnego dostępu, które były uruchomione na komputerze dodanym do wykluczeń i które były uruchomione przed uruchomieniem Kaspersky Endpoint Security for Windows, zakończ i ponownie

rozpocznij sesję zdalnego dostępu lub ponownie uruchom komputer, na którym zainstalowano Kaspersky Endpoint Security for Windows.

- Jeśli [zadanie aktualizacji jest uruchamiane z uprawnieniami określonego konta użytkownika](#), łaty produktu nie zostaną pobrane podczas aktualizacji ze źródła wymagającego autoryzacji.
- Aplikacja może nie zostać uruchomiona w wyniku słabej wydajności systemu. Aby rozwiązać ten problem, użyj opcji Ready Boot lub zwiększ limit czasu dla systemu operacyjnego i uruchamiania usług.
- Aplikacja nie działa w trybie awaryjnym.
- Aby upewnić się, że Kaspersky Endpoint Security for Windows w wersjach 11.5.0 i 11.6.0 może działać poprawnie z oprogramowaniem Cisco AnyConnect, musisz zainstalować Moduł Compliance w wersji 4.3.183.2048 lub nowszej. Zapoznaj się z informacjami na temat kompatybilności z Cisco Identity Services Engine w [dokumentacji Cisco](#).
- Nie można zagwarantować, że Kontrola audio będzie działała, aż do pierwszego ponownego uruchomienia po zainstalowaniu aplikacji.
- W Konsoli administracyjnej, w ustawieniach Ochrony przed włamaniami, w oknie konfigurowania uprawnień aplikacji przycisk **Usuń** jest niedostępny. Możesz usunąć aplikację z grupy zaufania z poziomu menu kontekstowego aplikacji.
- W lokalnym interfejsie aplikacji, w ustawieniach Ochrony przed włamaniami uprawnienia aplikacji i chronione zasoby nie są dostępne do przejrzania, jeśli komputer jest zarządzany przez zasadę. Przewijanie, wyszukiwanie, filtrowanie i inne kontrolki okna są niedostępne. Uprawnienia aplikacji możesz przejrzeć we właściwościach zasady, w konsoli Kaspersky Security Center Console.
- Gdy włączone jest tworzenie plików śledzenia z rotacją, pliki śledzenia nie są tworzone dla komponentu AMSI i wtyczki programu Outlook.
- Pliki śledzenia wydajności nie mogą zostać ręcznie zebrane w Windows Server 2008.
- Pliki śledzenia wydajności dla typu śledzenia „Ponowne uruchomienie” nie są obsługiwane.
- Zapisywanie zrzutu pamięci nie jest obsługiwane dla procesów pico.
- Zadanie sprawdzania dostępności KSN nie jest już obsługiwane.
- Wyłączenie opcji „Wyłącz możliwość zewnętrznego zarządzania usługami systemowi” nie zezwoli na zatrzymanie usługi aplikacji, która została zainstalowana z parametrem AMPPL=1 (domyślnie, wartość parametru jest ustawiona na 1, począwszy od systemu operacyjnego Windows 10RS2). Parametr AMPPL z wartością 1 włącza korzystanie z technologii procesów ochrony dla usługi produktu.
- Aby uruchomić skanowanie obiektów dla folderu, użytkownik, który uruchomił skanowanie obiektów, musi posiadać uprawnienia do odczytu atrybutów tego folderu. W przeciwnym razie skanowanie obiektów dla folderu będzie niemożliwe i zakończy się błędem.
- Jeśli reguła skanowania zdefiniowana w zasadzie zawiera ścieżkę bez znaku `\` na końcu, na przykład, `C:\folder1\folder2`, skanowanie zostanie uruchomione dla ścieżki `C:\folder1\`.
- Podczas aktualizowania aplikacji z wersji 11.1.0 do 11.7.0, zostaną przywrócone domyślne ustawienia Ochrony AMSI.
- Jeśli korzystasz z zasad ograniczeń oprogramowania (SRP), komputer może się nie załadować (czarny ekran). Zalecana jest zmiana ustawień SRP w następujący sposób: ustaw wartość **Wszystkie pliki oprogramowania oprócz bibliotek (takich jak DLL)** dla parametru **Zastosuj zasady ograniczeń**

oprogramowania do następujących obiektów i dodaj reguły z poziomem ochrony **Nieograniczone** dla ścieżek do plików aplikacji (C:\Program Files\Common Files\Kaspersky Lab i C:\Program Files\Kaspersky Lab). Więcej informacji na temat korzystania z SRP znajdziesz w [dokumentacji firmy Microsoft](#).

- Zarządzanie ustawieniami wtyczki dla programu Outlook za pośrednictwem API Rest nie jest obsługiwane.
- Ustawienia uruchamiania zadania dla określonego użytkownika nie mogą zostać przesłane między urządzeniami za pośrednictwem pliku konfiguracyjnego. Po zastosowaniu ustawień z pliku konfiguracyjnego, ręcznie określ nazwę użytkownika i hasło.
- Po zainstalowaniu aktualizacji, zadanie sprawdzania integralności nie będzie działało, aż system nie zostanie uruchomiony ponownie w celu zastosowania aktualizacji.
- Jeśli poziom śledzenia plików z rotacją zostanie zmieniony za pośrednictwem narzędzia do zdalnej diagnostyki, Kaspersky Endpoint Security for Windows niepoprawnie wyświetli pustą wartość dla poziomu śledzenia. Jednakże pliki śledzenia zostaną zapisane zgodnie z poprawnym poziomem śledzenia. Jeśli poziom śledzenia plików z rotacją zostanie zmieniony za pośrednictwem interfejsu lokalnego aplikacji, poziom śledzenia zostanie poprawnie zmodyfikowany, ale narzędzie do zdalnej diagnostyki będzie niepoprawnie wyświetlało poziom śledzenia, które zostało ostatnio zdefiniowane przez narzędzie. To może sprawić, że administrator nie będzie musiał aktualizować informacji o bieżącym poziomie śledzenia, a odpowiednie informacje mogą nie znajdować się w plikach śledzenia, jeśli użytkownik ręcznie zmieni poziom śledzenia w lokalnym interfejsie aplikacji.
- W interfejsie lokalnym ustawienia ochrony hasłem nie zezwalają na zmianę nazwy konta administratora (domyślnie KLAdmin). Aby zmienić nazwę konta administratora musisz wyłączyć Ochronę hasłem, a następnie włączyć Ochronę hasłem i określić nową nazwę konta administratora.
- Kaspersky Endpoint Security monitoruje ruch sieciowy http, który jest zgodny ze standardami RFC 2616, RFC 7540, RFC 7541, RFC 7301. Jeśli Kaspersky Endpoint Security wykryje inny format wymiany danych w ruchu HTTP, aplikacja blokuje to połączenie, aby zapobiec pobieraniu szkodliwych plików z internetu.
- Podczas skanowania połączenia szyfrowanego Kaspersky Endpoint Security wymusza protokół HTTP/1.
- Nie możesz przeskanować obiektu poddanego kwarantannie w wyniku działania zadania [Przenieś plik do Kwarantanny](#).
- Kaspersky Endpoint Security nie uruchamia zadań [Skanowanie IOC](#) na dyskach sieciowych, jeśli ścieżka do folderu we właściwościach zadania rozpoczyna się od litery dysku. Kaspersky Endpoint Security obsługuje tylko format ścieżki UNC dla zadań [Skanowanie IOC](#) na dyskach sieciowych. Na przykład:
\\server\shared_folder.
- [Importowanie pliku konfiguracyjnego aplikacji](#) zakończy się błędem, jeśli ustawienie [integracji z Kaspersky Sandbox](#) zostanie włączone w pliku konfiguracyjnym. Przed wyeksportowaniem ustawień aplikacji wyłącz Kaspersky Sandbox. Następnie wykonaj procedurę eksportu/importu. Po zaimportowaniu pliku konfiguracyjnego włącz Kaspersky Sandbox.
- Jeśli wskaźnik naruszeń bezpieczeństwa został wykryty podczas wykonywania zadania [Skanowanie IOC](#), aplikacja podda kwarantannie plik tylko dla warunku FileItem. Poddawanie pliku kwarantannie dla innych warunków nie jest obsługiwane.
- Nie można poddać kwarantannie mechanizmu Alternate Data Stream (ADS), który jest większy niż 4 MB. Kaspersky Endpoint Security pomija takie ADS bez powiadamiania użytkownika.
- Aby zarządzać szczegółami alertów, potrzebujesz wtyczki webowej dla Kaspersky Endpoint Security for Windows 11.7.0 lub nowszej. Szczegóły alertów są potrzebne dla rozwiązania [Endpoint Detection and Response](#) (EDR Optimum i EDR Expert). Szczegóły dotyczące detekcji są dostępne jedynie w Kaspersky Security Center Web Console i Kaspersky Security Center Cloud Console.

- Aplikacja Kaspersky Endpoint Security, gdy jest zainstalowana na serwerze Windows Server 2019, jest niekompatybilna z Docker. Zdalne instalowanie kontenerów Docker na komputerze z Kaspersky Endpoint Security powoduje awarię (BSOD).

Słownik

Agent autoryzacji

Interfejs umożliwiający przeprowadzenie procesu autoryzacji w celu uzyskania dostępu do zaszyfrowanych dysków twardech i załadowania systemu operacyjnego po zaszyfrowaniu dysku twardego.

Agent sieciowy

Składnik Kaspersky Security Center umożliwiający interakcję Serwera administracyjnego z aplikacjami firmy Kaspersky zainstalowanymi na określonym węźle sieciowym (stacji roboczej lub serwerze). Ten komponent jest wspólny dla wszystkich aplikacji firmy Kaspersky działających pod systemem Windows. Dla aplikacji działających pod innymi systemami operacyjnymi przeznaczone są dedykowane wersje Agenta sieciowego.

Aktywny klucz

Klucz, który jest aktualnie używany przez aplikację.

Antywirusowe bazy danych

Bazy danych zawierające informacje o zagrożeniach ochrony komputera znane specjalistom z Kaspersky w momencie opublikowania baz danych. Sygnatury antywirusowych baz danych pomagają wykrywać szkodliwy kod w skanowanych obiektach. Antywirusowe bazy danych są tworzone przez specjalistów z Kaspersky i aktualizowane co godzinę.

Archiwum

Jeden lub kilka plików spakowanych w jeden skompresowany plik. Do spakowania i wypakowania danych potrzebna jest specjalna aplikacja zwana archiwizatorem.

Baza adresów phishingowych

Lista adresów internetowych, które specjaliści z Kaspersky określili jako związane z phishingiem. Baza danych jest regularnie aktualizowana i jest częścią pakietu dystrybucyjnego aplikacji Kaspersky.

Baza danych szkodliwych adresów internetowych

Lista adresów internetowych o potencjalnie niebezpiecznej zawartości. Lista jest tworzona przez specjalistów z Kaspersky. Lista ta jest regularnie aktualizowana oraz znajduje się w pakiecie dystrybucyjnym aplikacji Kaspersky.

Certyfikat licencji

Dokument, który jest dostarczany użytkownikowi wraz z plikiem klucza lub kodem aktywacyjnym. Zawiera informacje o licencji nadanej użytkownikowi.

Fałszywy alarm

Fałszywy alarm występuje wtedy, gdy aplikacja Kaspersky uzna niezainfekowany plik za zainfekowany, gdyż sygnatura pliku przypomina sygnaturę wirusa.

Grupa administracyjna

Zbiór urządzeń posiadających takie same role i zainstalowany zestaw aplikacji Kaspersky. Urządzenia są grupowane, aby można było nimi wygodnie zarządzać jak pojedynczą jednostką. Grupa może zawierać w sobie inne grupy. Możliwe jest utworzenie profili grupowych i zadań grupowych dla każdej zainstalowanej aplikacji w grupie.

IOC

Wskaźnik naruszeń bezpieczeństwa Zestaw danych dotyczących szkodliwego obiektu lub aktywności.

Klucz dodatkowy

Klucz, który daje prawo do korzystania z aplikacji, chociaż nie jest on aktualnie w użyciu.

Leczenie

Metoda przetwarzania zainfekowanych obiektów skutkująca pełnym lub częściowym odzyskaniem danych. Nie każdy zainfekowany obiekt może zostać wyleczony.

Maska

Reprezentacja nazwy i rozszerzenia pliku przy użyciu symboli wieloznacznych.

Miski plików mogą zawierać dowolne znaki dozwolone w nazwach plików oraz symbole wieloznaczne:

- Znak ***** (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: **** i **/** (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:**.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
- Dwa występujące po sobie znaki ***** zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: **** i **/** (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na

przykład, maska `C:\Folder***.txt` będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie `Folder` i w jego podfolderach. Maskę musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maskę `C:***.txt` nie jest ważną maską. Maskę `**` jest dostępna tylko do tworzenia wykluczeń ze skanowania.

- Znak `?` (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: `\` i `/` (separatorzy nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska `C:\Folder\???.txt` będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie `Folder`, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.

Obiekt OLE

Załączony plik lub plik wbudowany w inny plik. Aplikacje firmy Kaspersky pozwalają na skanowanie obiektów OLE w poszukiwaniu wirusów. Na przykład, gdy dokument Microsoft Office Word zawiera tabelę Microsoft Office Excel®, będzie ona skanowana jako obiekt OLE.

Obszar ochrony

Obiekty, które są cały czas skanowane przez Podstawową ochronę przed zagrożeniami, gdy jest ona włączona. Obszary ochrony różnych modułów mają odmienne właściwości.

Obszar skanowania

Obiekty, które są skanowane przez Kaspersky Endpoint Security podczas uruchamiania zadania skanowania.

OpenIOC

Otwarty standard opisów Wskaźników naruszeń bezpieczeństwa (IOC) oparty na XML i zawierający ponad 500 różnych Wskaźników naruszeń bezpieczeństwa.

Plik infekowalny

Plik, który ze względu na swoją strukturę lub format może zostać użyty przez hakerów jako "kontener" do przechowywania i rozprzestrzeniania szkodliwego kodu. Zazwyczaj chodzi tu o pliki wykonywalne o rozszerzeniach, takich jak `.com`, `.exe` i `.dll`. Istnieje dość wysokie ryzyko wprowadzenia szkodliwego kodu do takich plików.

Plik IOC

Plik zawierający zestaw wskaźników naruszeń bezpieczeństwa (IOC), które aplikacja próbuje dopasować do licznika wykryć. Prawdopodobieństwo wykrycia może być wyższe, jeśli w wyniku skanowania dla obiektu znaleziono dokładne dopasowania z kilkoma plikami IOC.

Przenośny menedżer plików

To jest aplikacja oferująca interfejs do pracy z zaszyfrowanymi plikami na dyskach wymiennych, gdy funkcja szyfrowania nie jest dostępna na komputerze.

Trusted Platform Module (moduł TPM)

Mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej.

Wystawca certyfikatu

Centrum certyfikacji, które wydało certyfikat.

Zadanie

Funkcje wykonywane przez aplikację firmy Kaspersky pod postacią zadań, na przykład: Ochrona plików w czasie rzeczywistym, Pełne skanowanie urządzenia, Aktualizacja baz danych.

Zainfekowany plik

Plik zawierający szkodliwy kod (kod znanego szkodliwego programu, który został wykryty podczas skanowania pliku). Kaspersky nie zaleca korzystania z takich plików, ponieważ mogą prowadzić do zainfekowania komputera.

Znormalizowana postać adresu zasobu sieciowego

Znormalizowana postać adresu zasobu sieciowego to tekstowa reprezentacja adresu zasobu sieciowego, uzyskana poprzez normalizację. Normalizacja to proces, w którym tekstowa reprezentacja adresu zasobu sieciowego zmienia się zgodnie z określonymi regułami (na przykład, wykluczenie portu połączenia, hasła i loginu użytkownika z reprezentacji adresu zasobu sieciowego; dodatkowo adres zasobu sieciowego jest zmieniany z dużych znaków na małe).

W kontekście działania składników ochrony celem normalizacji adresu zasobu sieciowego jest pominięcie kolejnych skanowań adresów stron internetowych, które mają różną składnię, a fizycznie są takie same.

Na przykład:

Nieznormalizowana postać adresu: `www.Example.com\.`

Znormalizowana postać adresu: `www.example.com.`

Dodatki

Ta sekcja zawiera informacje uzupełniające treść dokumentu.

Dodatek 1. Ustawienia aplikacji

Do skonfigurowania Kaspersky Endpoint Security można użyć [zasady](#), [zadań](#) lub [interfejsu aplikacji](#). Szczegółowe informacje o komponentach aplikacji są dostępne w odpowiednich sekcjach.

Ochrona plików

Komponent Ochrona plików umożliwia uniknięcie infekcji systemu plików komputera. Domyślnie, składnik Ochrona plików na stałe znajduje się w pamięci RAM komputera. Składnik skanuje pliki na wszystkich dyskach komputera, a także na podłączonych dyskach. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, [usługi w chmurze Kaspersky Security Network](#) i analizy heurystycznej.

Komponent skanuje pliki otwierane przez użytkownika lub aplikację. Jeśli zostanie wykryty szkodliwy plik, Kaspersky Endpoint Security blokuje operację na pliku. Następnie aplikacja leczy lub usuwa szkodliwy plik, w zależności od ustawień komponentu Ochrona plików.

Podczas próby uzyskania dostępu do pliku, którego zawartości są przechowywane w chmurze OneDrive, Kaspersky Endpoint Security pobierze i przeskanuje zawartości plików.

Ustawienia komponentu Ochrona plików

Parametr	Opis
Poziom ochrony <i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i>	<p>Dla modułu Ochrona plików program Kaspersky Endpoint Security można zastosować różne grupy ustawień. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane <i>poziomami ochrony</i>.</p> <ul style="list-style-type: none">• Wysoki. Jeśli wybrano ten poziom ochrony plików, moduł Ochrona plików będzie dokładnie kontrolować wszystkie otwierane, zapisywane i uruchamiane pliki. Komponent Ochrona plików skanuje wszystkie typy plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Moduł ten skanuje także archiwa, pakiety instalacyjne i osadzone obiekty OLE.• Zalecany. Ten poziomy ochrony plików jest zalecany przez specjalistów z Kaspersky Lab. Komponent Ochrona plików skanuje wszystkie formaty plików na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera, a także osadzonych obiektów OLE. Moduł Ochrona plików nie skanuje archiwów oraz pakietów instalacyjnych.• Niski. Ustawienia tego poziomu ochrony plików zapewniają maksymalną prędkość skanowania. Komponent Ochrona plików skanuje tylko pliki z określonymi rozszerzeniami na wszystkich dyskach twardych, dyskach wymiennych i dyskach sieciowych komputera. Moduł Ochrona plików nie skanuje plików złożonych.
Typy plików	Wszystkie pliki. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanować wszystkie pliki bez wyjątku (wszystkie formaty i rozszerzenia).

<p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Pliki skanowane według formatu. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował tylko infekowalne pliki . Przed rozpoczęciem skanowania antywirusowego pliku analizowany jest jego wewnętrzny nagłówek w celu rozpoznania formatu (np. .txt, .doc, .exe). Skanowanie wyszukuje także pliki z określonymi rozszerzeniami plików.</p> <p>Pliki skanowane według rozszerzenia. Jeżeli wybierzesz tę opcję, Kaspersky Endpoint Security będzie skanował tylko infekowalne pliki . Format pliku będzie określany w oparciu o jego rozszerzenie.</p>
<p>Obszar modułu Ochrona plików</p>	<p>Zawiera obiekty skanowane przez moduł Ochrona plików. Skanowanym obiektem może być dysk twardy, nośnik wymienny, dysk sieciowy, folder, plik lub kilka plików zdefiniowanych według maski.</p> <p>Domyślnie Ochrona plików skanuje pliki uruchamiane na dyskach twardych, dyskach wymiennych i dyskach sieciowych. Obszar ochrony dla tych obiektów nie może zostać zmieniony ani usunięty. Możesz także wykluczyć obiekt (np. nośniki wymienne) ze skanowań.</p>
<p>Uczenie maszynowe i analiza sygnatur</p> <p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Metoda uczenia maszynowego i analiza sygnatur używa baz danych Kaspersky Endpoint Security, które zawierają opisy znanych zagrożeń oraz metody ich neutralizowania. Ochrona korzystająca z tej metody zapewnia minimalny dopuszczalny poziom ochrony.</p> <p>W oparciu o zalecenia ekspertów z Kaspersky, uczenie maszynowe i analiza sygnatur jest zawsze włączona.</p>
<p>Analiza heurystyczna</p> <p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa.</p> <p>Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.</p>
<p>Działanie podejmowane w przypadku wykrycia zagrożenia</p>	<p>Wylecz; usuń, jeśli leczenie nie jest możliwe. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeżeli leczenie nie powiedzie się, Kaspersky Endpoint Security usunie pliki.</p> <p>Wylecz; blokuje, jeśli leczenie nie jest możliwe. Jeśli wybrano tę opcję, Kaspersky Endpoint Security automatycznie podejmuje próbę wyleczenia wszystkich zainfekowanych plików, które zostały wykryte. Jeśli leczenie nie jest możliwe, Kaspersky Endpoint Security doda informacje o wykrytych zainfekowanych plikach do listy aktywnych zagrożeń.</p> <p>Blokuj. Jeśli wybrano tę opcję, moduł Ochrona plików automatycznie zablokuje wszystkie zainfekowane pliki, bez podjęcia próby ich wyleczenia.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Przed próbą wyleczenia lub usunięcia zainfekowanego pliku, Kaspersky Endpoint Security utworzy kopię zapasową pliku w przypadku, gdy potrzebujesz przywrócić plik lub jeśli może zostać wyleczony w przyszłości.</p> </div>

Skanuj tylko nowe i zmienione pliki	<p>Skanuje tylko nowe pliki oraz pliki, które zostały zmodyfikowane od ostatniego skanowania. To pomaga skrócić czas skanowania. Ten tryb jest stosowany zarówno do plików prostych, jak i złożonych.</p>
Skanuj archiwa	<p>Skanuje archiwa w następujących formatach: RAR, ARJ, ZIP, CAB, LHA, JAR i ICE. Kaspersky Endpoint Security skanuje archiwa nie tylko według rozszerzenia, ale także według formatu.</p>
Skanuj pakiety dystrybucyjne	<p>To pole włącza/wyłącza skanowanie pakietów dystrybucyjnych firm trzecich.</p>
Skanuj pliki w formatach Microsoft Office	<p>Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty.</p>
Nie rozpakowuj dużych plików złożonych	<p>Jeżeli to pole jest zaznaczone, Kaspersky Endpoint Security nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość.</p> <p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki złożone o wszystkich rozmiarach.</p> <div data-bbox="416 752 1493 875" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.</p> </div>
Rozpakowywanie plików złożonych w tle	<p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security oferuje dostęp do plików złożonych, które mają większy rozmiar niż wartość określona przed skanowaniem tych plików. W tym przypadku Kaspersky Endpoint Security rozpakowuje i skanuje pliki złożone w tle.</p> <p>Kaspersky Endpoint Security oferuje dostęp do plików złożonych, których rozmiar jest mniejszy niż ta wartość dopiero po rozpakowaniu i przeskanowaniu tych plików.</p> <p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security oferuje dostęp do plików złożonych dopiero po rozpakowaniu i przeskanowaniu plików dowolnego rozmiaru.</p>
Tryb skanowania <i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i>	<div data-bbox="416 1323 1493 1447" style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Kaspersky Endpoint Security skanuje pliki, do których dostęp uzyskał użytkownik, system operacyjny lub aplikacja uruchomiona z poziomu konta użytkownika.</p> </div> <p>Tryb smart. W tym trybie Ochrona plików skanuje obiekt w oparciu o analizę akcji podejmowanych na obiekcie. Na przykład, jeżeli wykorzystywany jest dokument Microsoft Office, Kaspersky Endpoint Security skanuje plik przy jego pierwszym otwieraniu i ostatnim zamykaniu. Wszystkie operacje wykonywane w międzyczasie, które nadpisują plik, nie są skanowane.</p> <p>Podczas dostępu i modyfikacji. W tym trybie moduł Ochrona plików skanuje obiekty za każdym razem, gdy są otwierane lub modyfikowane.</p> <p>Podczas dostępu. W tym trybie moduł Ochrona plików skanuje obiekty podczas ich otwierania.</p> <p>Podczas wykonywania. W tym trybie moduł Ochrona plików skanuje obiekty jedynie podczas ich uruchamiania.</p>
Technologia iSwift	<p>Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczanie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz modyfikacje ustawień skanowania. Technologia iSwift stanowi rozwinięcie technologii iChecker dla systemu plików NTFS.</p>

<p>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</p>	
<p>Technologia iChecker (dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</p>	<p>Technologia ta pozwala na zwiększenie szybkości skanowania poprzez wykluczenie pewnych plików ze skanowania. Pliki są wykluczane ze skanowania przy użyciu specjalnego algorytmu uwzględniającego datę publikacji baz danych Kaspersky Endpoint Security, datę ostatniego skanowania pliku oraz wszelkie modyfikacje ustawień skanowania. Ograniczeniem technologii iChecker jest fakt, że nie obsługuje ona plików o dużym rozmiarze oraz może być wykorzystana wyłącznie dla plików, których struktura jest rozpoznawana przez aplikację (na przykład: EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP i RAR).</p>
<p>Wstrzymaj moduł Ochrona plików (dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</p>	<p>To powoduje tymczasowe i automatyczne wstrzymanie działania modułu Ochrona plików o określonym czasie lub podczas pracy z określonymi aplikacjami.</p>

Ochrona WWW

Komponent Ochrona WWW zapobiega pobieraniu szkodliwych plików z internetu, a także blokuje szkodliwe i phishingowe strony internetowe. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, [usługi w chmurze Kaspersky Security Network](#) i analizy heurystycznej.

Kaspersky Endpoint Security skanuje ruch HTTP, HTTPS i FTP. Kaspersky Endpoint Security skanuje adresy internetowe i adresy IP. Możesz [określić porty monitorowane przez Kaspersky Endpoint Security](#) lub wybrać wszystkie porty.

Dla monitorowania ruchu HTTPS należy [włączyć skanowanie zaszyfrowanych połączeń](#).

Gdy użytkownik próbuje otworzyć złośliwą lub phishingową stronę internetową, Kaspersky Endpoint Security zablokuje dostęp i wyświetli ostrzeżenie (patrz rysunek poniżej).



Dostęp zabroniony

Żądany adres internetowy nie może zostać pobrany

http://kl-test-page.avp.ru/new_ksn_samples/AVS_RISKWARE-KSN_BAD.exe

Powód:

obiekt jest zainfekowany przez [UDS:DangerousObject.Multi.Generic](#)

Komunikat wygenerowano: 10/8/2020 10:10:30 PM

kaspersky

Wiadomość o odmowie dostępu do strony internetowej

Ustawienia komponentu Ochrona WWW

Parametr	Opis
Poziom ochrony <i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i>	<p>Dla modułu Ochrona WWW program Kaspersky Endpoint Security można zastosować różne grupy ustawień. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane <i>poziomami ochrony</i>.</p> <ul style="list-style-type: none">• Wysoki. Poziom ochrony, zgodnie z którym Ochrona WWW przeprowadza skanowanie ruchu sieciowego, odbieranego przez komputer poprzez protokoły HTTP i FTP, na maksymalnym poziomie. Ochrona WWW szczegółowo skanuje wszystkie obiekty ruchu sieciowego, używając pełnego zestawu baz danych aplikacji, a także przeprowadza najbardziej szczegółową analizę heurystyczną.• Zalecany. Jest to poziom ochrony zapewniający optymalną równowagę pomiędzy wydajnością Kaspersky Endpoint Security a ochroną ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na średnim poziomie. Ten poziom ochrony ruchu sieciowego jest zalecany przez specjalistów z Kaspersky.• Niski. Ustawienia tego poziomu ochrony ruchu sieciowego zapewniają maksymalną prędkość skanowania ruchu sieciowego. Ochrona WWW wykonuje analizę heurystyczną na niskim poziomie.
Działanie podejmowane w przypadku wykrycia zagrożenia	<p>Zablokuj pobranie. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Ochrona WWW zablokuje dostęp do obiektu i wyświetli komunikat w przeglądarce.</p> <p>Informuj. Jeśli ta opcja jest zaznaczona, a zainfekowany obiekt zostanie wykryty w ruchu sieciowym, Kaspersky Endpoint Security pozwala na pobranie tego obiektu na komputer, ale dodaje informacje o zainfekowanym obiekcie do listy aktywnych zagrożeń.</p>
Sprawdź adres internetowy zgodnie z bazą szkodliwych	<p>Skanowanie odnośników do określenia, czy znajdują się w bazie danych szkodliwych odnośników pozwoli na śledzenie stron internetowych, które zostały dodane do listy zablokowanych. Baza danych szkodliwych adresów internetowych, która została</p>

<p>adresów internetowych</p> <p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p>stworzona przez Kaspersky, znajduje się w pakiecie instalacyjnym aplikacji i jest aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.</p>
<p>Użyj analizy heurystycznej</p> <p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa.</p> <p>Jeśli ruch sieciowy jest skanowany w poszukiwaniu wirusów i innych aplikacji, które stwarzają zagrożenie, analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.</p>
<p>Sprawdź adres internetowy zgodnie z bazą phishingowych adresów internetowych</p> <p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Baza danych phishingowych adresów internetowych zawiera adresy internetowe obecnie znanych stron wykorzystywanych przy atakach phishingowych. Kaspersky uzupełnia tę bazę odnośników phishingowych o adresy uzyskane z międzynarodowej organizacji znanej jako Anti-Phishing Working Group. Baza danych adresów phishingowych znajduje się w pakiecie instalacyjnym aplikacji, jest również aktualizowana wraz z uaktualnieniami baz danych Kaspersky Endpoint Security.</p>
<p>Nie skanuj ruchu sieciowego z zaufanych adresów internetowych</p>	<p>Jeśli pole jest zaznaczone, moduł Ochrona WWW nie skanuje zawartości stron internetowych, których adresy znajdują się na liście zaufanych adresów internetowych. Do listy zaufanych adresów internetowych możesz dodać określony adres i maskę adresu strony internetowej.</p>

Ochrona poczty

Ochrona poczty skanuje załączniki odbieranych i wysyłanych wiadomości e-mail w poszukiwaniu wirusów i innych zagrożeń. Komponent skanuje również wiadomości w poszukiwaniu szkodliwych i phishingowych odnośników. Domyślnie, składnik Ochrona poczty na stałe znajduje się w pamięci RAM komputera i skanuje wszystkie wiadomości otrzymane lub wysłane za pomocą protokołów POP3, SMTP, IMAP lub NNTP lub klienta poczty Microsoft Office Outlook (MAPI). Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, [usługi w chmurze Kaspersky Security Network](#) i analizy heurystycznej.

Komponent Ochrona poczty nie skanuje wiadomości, jeśli klient poczty jest otwarty w przeglądarce.

Jeśli w załączniku zostanie wykryty szkodliwy plik, Kaspersky Endpoint Security zmieni nazwę tematu wiadomości w następujący sposób: [Wiadomość jest zainfekowana] <temat wiadomości> lub [Usunięto zainfekowany obiekt] <temat wiadomości>.

Składnik współdziała z klientami poczty e-mail zainstalowanymi na komputerze. W przypadku klienta poczty Microsoft Office Outlook dostarczane jest [rozszerzenie z dodatkowymi parametrami](#). Rozszerzenie Ochrony poczty jest integrowane z programem pocztowym Microsoft Office Outlook w trakcie instalacji Kaspersky Endpoint Security.

Ustawienia komponentu Ochrona poczty

Parametr	Opis
<p>Poziom ochrony (dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</p>	<p>Dla modułu Ochrona poczty program Kaspersky Endpoint Security stosuje różne grupy ustawień. Te grupy ustawień, które są przechowywane w aplikacji, są nazywane <i>poziomami ochrony</i>.</p> <ul style="list-style-type: none"> • Wysoki. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty szczegółowo skanuje wiadomości e-mail. Ochrona poczty skanuje przychodzące i wychodzące wiadomości e-mail, a także przeprowadza szczegółową analizę heurystyczną. Wysoki poziom ochrony poczty jest zalecany dla środowisk wysokiego ryzyka. Przykładem takiego środowiska jest korzystanie z darmowego serwera pocztowego, który nie jest chroniony żadnym systemem antywirusowym. • Zalecany. Jest to poziom ochrony zapewniający optymalną równowagę pomiędzy wydajnością Kaspersky Endpoint Security a ochroną poczty. Ochrona poczty skanuje wiadomości przychodzące i wychodzące, a także przeprowadza analizę heurystyczną na średnim poziomie intensywności. Ten poziom ochrony ruchu pocztowego jest zalecany przez specjalistów z Kaspersky. • Niski. Jeśli wybrany jest ten poziom ochrony, moduł Ochrona poczty skanuje tylko wiadomości przychodzące, wykonuje analizę heurystyczną na niskim poziomie, a także nie skanuje archiwów załączonych do wiadomości e-mail. Na tym poziomie moduł Ochrona poczty skanuje wiadomości z maksymalną prędkością i używa minimalnej ilości zasobów systemu operacyjnego. Niski poziom ochrony jest zalecany podczas pracy w dobrze chronionym środowisku. Przykładem takiego środowiska może być firmowa sieć LAN ze scentralizowaną ochroną poczty.
<p>Działanie podejmowane w przypadku wykrycia zagrożenia</p>	<p>Wylecz; usuń, jeśli leczenie nie jest możliwe. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej lub wychodzącej, Kaspersky Endpoint Security podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, Kaspersky Endpoint Security usunie zainfekowany obiekt. Kaspersky Endpoint Security dodaje do tematu wiadomości informacje o wykonanym działaniu: [Usunięto zainfekowany obiekt] <temat wiadomości>.</p> <p>Wylecz; blokuj, jeśli leczenie nie jest możliwe. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, Kaspersky Endpoint Security podejmie próbę wyleczenia wykrytego obiektu. Użytkownik będzie mógł uzyskać dostęp do wiadomości z bezpiecznym załącznikiem. Jeśli obiektu nie można wyleczyć, Kaspersky Endpoint Security doda ostrzeżenie do tematu wiadomości: [Wiadomość zainfekowana] <temat wiadomości>. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeśli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, Kaspersky Endpoint Security podejmie próbę wyleczenia wykrytego obiektu. Jeśli obiektu nie można wyleczyć, Kaspersky Endpoint Security zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.</p>

	<p>Blokuj. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości przychodzącej, Kaspersky Endpoint Security doda ostrzeżenie do tematu wiadomości: [Wiadomość zainfekowana] <temat wiadomości>. Użytkownik będzie mógł uzyskać dostęp do wiadomości z oryginalnym załącznikiem. Jeżeli zainfekowany obiekt zostanie wykryty w wiadomości wychodzącej, Kaspersky Endpoint Security zablokuje transmisję wiadomości, a klient poczty wyświetli błąd.</p>
<p>Obszar ochrony</p> <p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p><i>Obszar ochrony</i> obejmuje obiekty, które komponent sprawdza podczas działania: Wiadomości odbierane i wysyłane lub Tylko wiadomości przychodzące.</p> <p>Aby chronić komputery, należy skanować tylko wiadomości przychodzące. Możesz włączyć skanowanie wiadomości wychodzących, aby zapobiec wysłaniu zainfekowanych plików w archiwach. Możesz także włączyć skanowanie wiadomości wychodzących, jeśli chcesz zapobiec wysłaniu plików w określonych formatach, na przykład plików audio i wideo.</p>
<p>Skanuj ruch POP3, SMTP, NNTP i IMAP</p>	<p>Pole to włącza/wyłącza skanowanie ruchu przesyłanego przez protokoły POP3, SMTP, NNTP i IMAP.</p>
<p>Włącz rozszerzenie Microsoft Outlook</p>	<p>Jeśli pole jest zaznaczone, skanowanie wiadomości przesyłanych poprzez protokoły POP3, SMTP, NNTP, IMAP jest włączone po stronie rozszerzenia zintegrowanego w Microsoft Outlook.</p> <p>Jeśli poczta jest skanowana przy użyciu rozszerzenia dla programu Microsoft Outlook, zalecane jest korzystanie z trybu buforowanego programu Exchange. Więcej informacji dotyczących trybu buforowanego programu Exchange oraz zalecenia dotyczące korzystania z tego trybu można znaleźć w Bazie wiedzy Microsoft.</p>
<p>Analiza heurystyczna</p> <p><i>(dostępne tylko w Konsoli administracyjnej (MMC) i w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Technologia została stworzona w celu wykrywania zagrożeń, które nie mogą zostać wykryte przy pomocy aktualnych baz danych aplikacji Kaspersky. Wykrywa pliki, które mogły zostać zainfekowane nieznanym wirusem lub modyfikacją znanego wirusa.</p> <p>Podczas skanowania plików lub szkodliwego kodu analizator heurystyczny wykonuje instrukcje w plikach wykonywalnych. Liczba instrukcji, które są wykonywane przez analizator heurystyczny, zależy od poziomu, który jest określony dla analizatora heurystycznego. Poziom szczegółowości analizy heurystycznej zapewnia równowagę pomiędzy dokładnością wyszukiwania nowych zagrożeń, poziomem obciążenia zasobów systemu operacyjnego oraz czasem trwania analizy heurystycznej.</p>
<p>Skanuj załączone archiwa</p>	<p>Skanuje archiwa w następujących formatach: RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Jeżeli podczas skanowania Kaspersky Endpoint Security wykryje w tekście wiadomości hasło do archiwum, hasło to zostanie wykorzystane do przeskanowania zawartości archiwum w poszukiwaniu szkodliwych aplikacji. W tym przypadku hasło nie zostaje zapisane. Archiwum jest rozpakowywane podczas skanowania. Jeśli podczas rozpakowywania wystąpi błąd aplikacji, można ręcznie usunąć rozpakowane pliki, które są zapisywane w następującej ścieżce: %systemroot%\temp. Pliki mają prefiks PR.</p> </div>
<p>Skanuj załączone pliki formatów pakietu Office</p>	<p>Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty.</p>
<p>Nie skanuj archiwów</p>	<p>Jeżeli pole jest zaznaczone, moduł Ochrona poczty wyklucza ze skanowania archiwa, załączone do wiadomości, których rozmiar przekracza określoną wartość. Jeżeli pole nie</p>

większych niż N MB	jest zaznaczone, moduł Ochrona poczty skanuje załączone archiwa o dowolnym rozmiarze.
Ogranicz czas sprawdzania archiwów do N s	Jeżeli pole jest zaznaczone, czas skanowania załączonych archiwów jest ograniczony.
Filtr załączników	<div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;">Filtr załączników nie jest stosowany do wychodzących wiadomości e-mail.</div> <p>Wyłącz filtrowanie. Jeśli ta opcja jest wybrana, Ochrona poczty nie filtruje plików załączonych do wiadomości e-mail.</p> <p>Zmień nazwy załączników określonych typów. Jeśli wybierzesz tę opcję, Ochrona poczty zastąpi ostatni znak rozszerzenia wykryty w załączonych plikach określonych typów znakiem podkreślenia (na przykład: attachment.doc_). Dlatego, aby otworzyć plik, użytkownik musi zmienić jego nazwę.</p> <p>Usuń załączniki wybranych typów. Jeśli ta opcja jest zaznaczona, Ochrona poczty usuwa załączone pliki określonych typów z wiadomości e-mail.</p> <p>Na liście masek plików możesz określić typy załączonych plików, których nazwy mają zostać zmienione lub które mają zostać usunięte z wiadomości e-mail.</p>

Ochrona sieci

Moduł Ochrona sieci bada przychodzący ruch sieciowy pod kątem aktywności typowych dla ataków sieciowych. Jeśli Kaspersky Endpoint Security wykryje próbę ataku sieciowego na komputerze użytkownika, zablokuje połączenie sieciowe z komputerem atakującym. Opisy znanych typów ataków sieciowych oraz sposoby ich zwalczania znajdują się w bazach danych programu Kaspersky Endpoint Security. Lista ataków sieciowych, wykrywanych przez komponent Ochrona sieci, jest uaktualniana podczas [aktualizacji baz danych i modułów aplikacji](#).

Ustawienia komponentu Ochrona sieci

Parametr	Opis
Traktuj skanowanie portów i "network flooding" jako ataki	<p><i>Zalewanie sieci</i> jest atakiem na zasoby sieciowe (takie jak serwery internetowe). Ten atak obejmuje wysyłanie dużej liczby żądań w celu przeciążenia przepustowości zasobów sieciowych. W takiej sytuacji użytkownicy nie mogą uzyskać dostępu do zasobów sieciowych organizacji.</p> <p>Atak <i>Skanowanie portów</i> obejmuje skanowanie portów UDP, portów TCP, a także usługi sieciowe komputera. Ten atak umożliwia atakującemu zidentyfikowanie stopnia podatności komputera przed przeprowadzeniem bardziej niebezpiecznych rodzajów ataków sieciowych. Skanowanie portów umożliwia atakującemu także zidentyfikowanie systemu operacyjnego na komputerze i wybranie odpowiednich ataków sieciowych dla tego systemu operacyjnego.</p> <p>Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security monitoruje ruch sieciowy do wykrywania następujących ataków dla. W przypadku wykrycia ataku aplikacja powiadamia użytkownika i wysyła odpowiednie zdarzenie do Kaspersky Security Center. Aplikacja dostarcza informacji o atakującym komputerze, co jest niezbędne do szybkiego reagowania na zagrożenia.</p>

	Możesz wyłączyć wykrywanie tych rodzajów ataków w przypadku, gdy niektóre z Twoich dozwolonych aplikacji wykonują działania typowe dla tych rodzajów ataków. Pomoże to w uniknięciu fałszywych alarmów.
Dodaj atakujący komputer do listy blokowanych komputerów na N min	<p>Jeśli pole jest zaznaczone, Ochrona sieci dodaje atakujący komputer do listy zablokowanych. Oznacza to, że komponent Ochrona sieci zablokuje na określony czas połączenie sieciowe z atakującym komputerem po pierwszej próbie ataku sieciowego. Ta blokada automatycznie chroni komputer użytkownika przed przyszłymi atakami sieciowymi pochodzącymi z tego samego adresu. Minimalny czas, przez jaki atakujący komputer będzie znajdować się na liście blokowanych, to jedna minuta. Maksymalny czas to 32 768 minut.</p> <p>W oknie Narzędzia Monitor sieci możesz przejrzeć listę blokowania.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Kaspersky Endpoint Security czyści listę blokowania, gdy aplikacja zostanie ponownie uruchomiona, a ustawienia Ochrony sieci zostaną zmienione.</p> </div>
Wykluczenia	<p>Lista zawiera adresy IP, z których Ochrona sieci nie blokuje ataków sieciowych.</p> <p>Aplikacja nie zapisuje informacji o atakach sieciowych pochodzących z adresów IP, które znajdują się na liście wykluczeń.</p>
Ochrona przed fałszowaniem adresu MAC	<i>Atak przez fałszowanie adresu MAC</i> obejmuje zmianę adresu MAC urządzenia sieciowego (karty sieciowej). W rezultacie osoba atakująca może przekierować dane wysłane do urządzenia na inne urządzenie i uzyskać dostęp do tych danych. Kaspersky Endpoint Security umożliwia blokowanie ataków przez fałszowanie adresu MAC i otrzymywanie powiadomień o atakach.

Zapora sieciowa

Zapora sieciowa blokuje nieautoryzowane połączenia z komputerem podczas pracy w internecie lub sieci lokalnej. Zapora sieciowa kontroluje również aktywność sieciową aplikacji na komputerze. Pozwala to chronić korporacyjną sieć LAN przed kradzieżą tożsamości i innymi atakami. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network i predefiniowanych *reguł sieciowych*.

Agent sieciowy jest używany do interakcji z Kaspersky Security Center. Zapora sieciowa automatycznie tworzy reguły sieciowe wymagane do działania aplikacji i Agenta sieciowego. W wyniku działania Zapora sieciowa otwiera kilka portów na komputerze. Które porty są otwarte w zależności od roli komputera (na przykład, punkt dystrybucji). Więcej informacji o portach, które zostaną otwarte na komputerze, można znaleźć w [pomocy dla Kaspersky Security Center](#).

Reguły sieciowe

Możesz skonfigurować reguły sieciowe na następujących poziomach:

- *Reguły pakietów sieciowych.* Reguły pakietów sieciowych nakładają ograniczenia na pakiety sieciowe, niezależnie od aplikacji. Takie reguły ograniczają ruch sieciowy wychodzący i przychodzący przez określone porty wybranego protokołu. Kaspersky Endpoint Security wstępnie zdefiniował reguły pakietów sieciowych z uprawnieniami zalecanymi przez ekspertów z Kaspersky.
- *Reguły sieciowe dla aplikacji.* Reguły sieciowe dla aplikacji nakładają ograniczenia na aktywność sieciową określonej aplikacji. W tym przypadku brane są pod uwagę cechy charakterystyczne pakietu sieciowego, a także aplikacja, dla której jest on przeznaczony lub która zainicjowała jego przesyłanie.

Kontrolowany dostęp aplikacji do zasobów systemu operacyjnego, procesów i danych osobowych jest zapewniany przez [komponent Ochrona przed włamaniami](#) przy użyciu *uprawnień aplikacji*.

Podczas pierwszego uruchomienia aplikacji Zapora sieciowa wykonuje następujące działania:

1. Sprawdza bezpieczeństwo aplikacji przy użyciu pobranych antywirusowych baz danych.
2. Sprawdza bezpieczeństwo aplikacji w Kaspersky Security Network.
Zalecane jest [uczestniczenie w Kaspersky Security Network](#), aby zapewnić bardziej efektywne działanie Zapory sieciowej.
3. Umieszcza aplikację w jednej z *grup zaufania*: Zaufane, Niski poziom ograniczeń, Wysoki poziom ograniczeń, Niezaufane.

[Grupa zaufania określa uprawnienia](#), do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.

Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania dla składników Zapora sieciowa i Ochrona przed włamaniami. Nie można zmienić grupy zaufania tylko dla Zapory sieciowej lub Ochrony przed włamaniami.

Jeśli odmówiłeś uczestnictwa w KSN lub nie ma sieci, Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od [ustawień modułu Ochrona przed włamaniami](#). Po otrzymaniu reputacji aplikacji od KSN, grupę zaufania można zmienić automatycznie.

4. Blokuje aktywność sieciową aplikacji w zależności od grupy zaufania. Na przykład, aplikacje z grupy Wysoki poziom ograniczeń nie mogą korzystać z żadnych połączeń sieciowych.

Przy następnym uruchomieniu aplikacji, Kaspersky Endpoint Security sprawdzi integralność aplikacji. Jeżeli aplikacja nie została zmieniona, moduł użyje dla niej bieżących reguł sieciowych. Jeżeli aplikacja została zmodyfikowana, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

Priorytety reguł sieciowych

Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli aktywność sieci zostanie dodana do kilku reguł, Zapora sieciowa reguluje aktywność sieciową zgodnie z regułą o najwyższym priorytecie.

Reguły pakietów sieciowych mają wyższy priorytet niż reguły sieciowe dla aplikacji. Jeżeli do tego samego typu aktywności sieciowej są zastosowane reguły pakietów sieciowych i reguły sieciowe dla aplikacji, będzie ona przetwarzana zgodnie z regułami pakietów sieciowych.

Reguły sieciowe dla aplikacji działają w następujący sposób: reguła sieciowa dla aplikacji obejmuje reguły dostępu oparte na stanie sieci: *publiczna*, *lokalna* lub *zaufana*. Na przykład, aplikacje z grupy zaufania Wysoki poziom ograniczeń domyślnie nie zezwalają na żadną aktywność sieciową w sieciach o wszystkich stanach. Jeśli dla pojedynczej aplikacji (aplikacji nadrzędnej) zostanie określona reguła sieciowa, procesy potomne innych aplikacji będą działać zgodnie z regułą sieciową aplikacji nadrzędnej. Jeśli nie istnieje reguła sieciowa dla aplikacji, procesy potomne będą działały zgodnie z regułą dostępu do sieci grupy zaufania aplikacji.

Na przykład, zabroniona jest jakakolwiek aktywność sieciowa w sieciach o wszystkich stanach dla wszystkich aplikacji, za wyjątkiem przeglądarki X. Jeśli rozpoczniesz instalację przeglądarki Y (proces potomny) z przeglądarki X (aplikacja nadrzędna), wówczas instalator przeglądarki Y uzyska dostęp do sieci i pobierze niezbędne pliki. Po instalacji przeglądarka Y będzie odmawiała jakichkolwiek połączeń sieciowych zgodnie z ustawieniami Zapory sieciowej. Aby zabronić aktywności sieciowej instalatora przeglądarki Y jako procesu potomnego, należy dodać regułę sieciową dla instalatora przeglądarki Y.

Stany połączenia sieciowego

Zapora sieciowa pozwala kontrolować aktywność sieciową w zależności od stanu połączenia sieciowego. Kaspersky Endpoint Security otrzymuje stan połączenia sieciowego z systemu operacyjnego komputera. Stan połączenia sieciowego w systemie operacyjnym jest ustawiany przez użytkownika podczas konfigurowania połączenia. Możesz [zmienić stan połączenia sieciowego w ustawieniach Kaspersky Endpoint Security](#). Zapora sieciowa będzie monitorować aktywność sieci w zależności od stanu sieci w ustawieniach Kaspersky Endpoint Security, a nie w systemie operacyjnym.

Połączenie sieciowe może mieć jeden z następujących typów stanu:

- **Sieć publiczna.** Sieć nie jest chroniona przez aplikacje antywirusowe, zapory sieciowe ani filtry (takie jak Wi-Fi w kawiarni). Podczas korzystania z komputera podłączonego do tego typu sieci Zapora sieciowa blokuje dostęp do plików i drukarek tego komputera. Użytkownicy z zewnątrz nie będą mogli również uzyskać dostępu do danych poprzez folder współdzielony oraz zdalnego dostępu do pulpitu tego komputera. Zapora sieciowa filtruje aktywność sieciową każdej aplikacji zgodnie z utworzoną dla niej regułą sieciową.

Domyślnie do internetu przypisywany jest stan *Sieć publiczna*. Nie możesz zmienić stanu przypisanego do internetu.

- **Sieć lokalna.** Sieć dla użytkowników z ograniczonym dostępem do plików i drukarek na tym komputerze (na przykład dla firmowej sieci LAN lub sieci domowej).
- **Sieć zaufana.** Bezpieczna sieć, w której komputer nie jest wystawiony na ataki lub nieautoryzowane próby dostępu do danych. Zapora sieciowa zezwala na dowolną aktywność sieciową w obrębie sieci o tym stanie.

Ustawienia komponentu Zapora sieciowa

Parametr	Opis
Reguły pakietów sieciowych	<p>Tabela zawierająca reguły pakietów sieciowych. Reguły pakietów sieciowych nakładają ograniczenia na pakiety sieciowe, niezależnie od aplikacji. Takie reguły ograniczają ruch sieciowy wychodzący i przychodzący przez określone porty wybranego protokołu.</p> <p>Tabela wyświetla predefiniowane reguły pakietów sieciowych, które są zalecane przez ekspertów z Kaspersky dla optymalnej ochrony ruchu sieciowego komputerów działających pod kontrolą systemów operacyjnych Microsoft Windows.</p> <p>Zapora sieciowa ustawia priorytet wykonania każdej reguły dla pakietu sieciowego. Zapora sieciowa przetwarza reguły w kolejności, w jakiej występują na liście reguł dla pakietów sieciowych (od góry do dołu). Zapora sieciowa odnajduje pierwszą regułę pakietu sieciowego odpowiadającą danemu połączeniu sieciowemu i stosuje ją, zezwalając na lub blokując aktywność sieciową. Następnie Zapora sieciowa ignoruje wszystkie kolejne reguły pakietów sieciowych dla określonego połączenia sieciowego.</p> <p>Reguły pakietów sieciowych mają wyższy priorytet niż reguły sieciowe dla aplikacji.</p>
Połączenia sieciowe	<p>Ta tabela zawiera informacje o połączeniach sieciowych wykrywanych na komputerze przez Zaporę sieciową.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Domyślnie do internetu przypisywany jest stan <i>Sieć publiczna</i>. Nie możesz zmienić stanu przypisanego do internetu.</p> </div>

<p>Reguły sieciowe</p>	<p>Aplikacje</p> <p>Tabela aplikacji kontrolowanych przez komponent Zapora sieciowa. Aplikacje są przypisywane do grup zaufania. Grupa zaufania określa prawa używane przez Kaspersky Endpoint Security podczas kontrolowania aktywności sieciowej aplikacji.</p> <p>Możesz wybrać aplikację z jednej listy wszystkich aplikacji zainstalowanych na komputerach pod kontrolą zasady i dodać aplikację do grupy zaufania.</p> <p>Reguły sieciowe</p> <p>Tabela reguł sieciowych dla aplikacji należących do grupy zaufania. Zgodnie z tymi regułami Zapora sieciowa reguluje aktywność sieciową aplikacji.</p> <p>Tabela wyświetla predefiniowane reguły sieciowe, które są zalecane przez ekspertów z Kaspersky. Te reguły sieciowe zostały dodane w celu optymalnej ochrony ruchu sieciowego komputerów z systemami operacyjnymi Windows. Nie można usunąć predefiniowanych reguł sieciowych.</p>
-------------------------------	--

Ochrona przed atakami BadUSB

Niektóre wirusy modyfikują oprogramowanie wbudowane urządzeń USB w celu zmylenia systemu operacyjnego do wykrywania urządzenia USB jako klawiatury. W wyniku tego działania wirus może wykonać polecenia z poziomu konta użytkownika, na przykład, w celu pobrania szkodliwego oprogramowania.

Komponent Ochrona przed atakami BadUSB zapobiega podłączeniu do komputera zainfekowanych urządzeń USB emulujących klawiaturę.

Po podłączeniu urządzenia USB do komputera i zidentyfikowaniu go przez system operacyjny jako klawiatury, aplikacja wyświetli pytanie o wprowadzenie kodu numerycznego, wygenerowanego przez aplikację, z poziomu tej klawiatury lub [Klawiatury ekranowej, jeśli jest dostępna](#) (patrz rysunek poniżej). Ta procedura jest znana jako autoryzacja klawiatury.

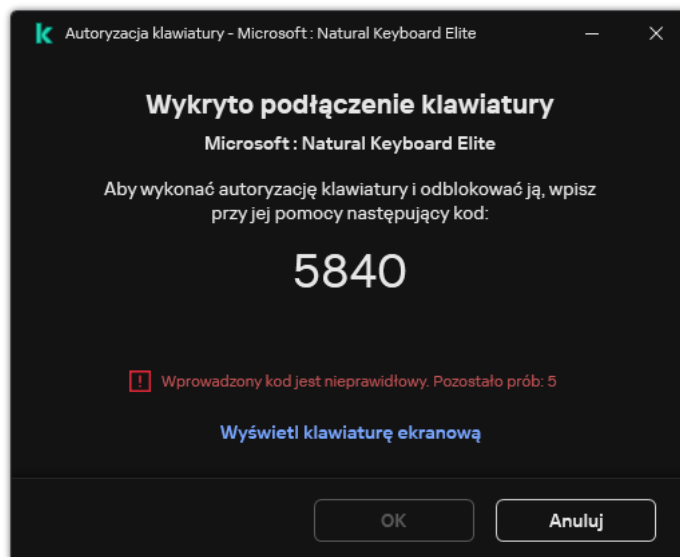
Jeśli kod zostanie wprowadzony poprawnie, aplikacja zapisze na liście zautoryzowanych klawiatur parametry identyfikujące klawiaturę - numer VID/PID, a także numer portu, do którego ta klawiatura została podpięta. Po ponownym podłączeniu klawiatury lub po ponownym uruchomieniu systemu nie ma konieczności powtarzania procesu autoryzacji klawiatury.

Jeśli zautoryzowana klawiatura zostanie podłączona do innego portu USB, aplikacja ponownie wyświetli pytanie o przeprowadzenie autoryzacji tej klawiatury.

Jeśli kod numeryczny zostanie wprowadzony niepoprawnie, aplikacja wygeneruje nowy kod. Możesz [skonfigurować liczbę prób wprowadzenia kodu numerycznego](#). Jeśli kod numeryczny zostanie wprowadzony niepoprawnie kilka razy lub okno autoryzacji klawiatury jest zamknięte (patrz rysunek poniżej), aplikacja zablokuje wprowadzenie z poziomu tej klawiatury. Po upływie czasu blokowania urządzenia USB lub ponownym uruchomieniu systemu operacyjnego, aplikacja ponownie wyświetli pytanie o przeprowadzenie autoryzacji klawiatury.

Aplikacja zezwoli na użycie zautoryzowanej klawiatury, a zablokuje klawiaturę, która nie została zautoryzowana.

Komponent Ochrona przed atakami BadUSB nie jest domyślnie instalowany. Jeśli potrzebujesz składnika Ochrona przed atakami BadUSB, możesz dodać ten składnik we właściwościach [pakietu instalacyjnego](#) przed zainstalowaniem aplikacji lub [zmienić dostępne składniki aplikacji](#) po zainstalowaniu aplikacji.



Autoryzacja klawiatury

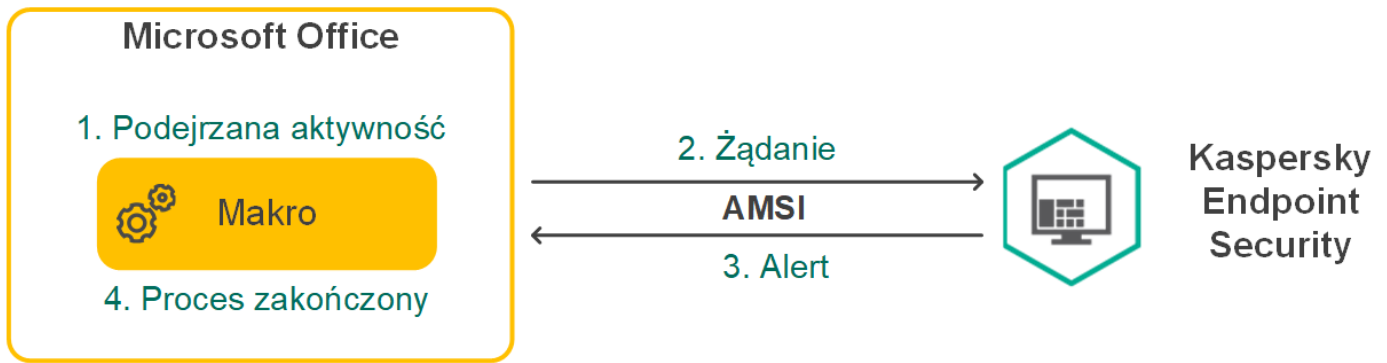
Ustawienia komponentu Ochrona przed atakami BadUSB

Parametr	Opis
Zabroń korzystania z Klawiatury ekranowej do autoryzacji urządzeń USB	Jeśli pole jest zaznaczone, aplikacja zablokuje użycie Klawiatury ekranowej podczas autoryzacji urządzenia USB, z poziomu którego nie można wpisać kodu autoryzacyjnego.
Maksymalna liczba prób autoryzacji urządzenia	Automatyczne blokowanie urządzenia USB, jeśli kod autoryzacyjny jest wprowadzany niepoprawnie określoną liczbę. Ważne wartości to 1 do 10. Na przykład, jeśli zezwolisz na 5 prób wprowadzenia kodu autoryzacyjnego, urządzenie USB zostanie zablokowane po piątej nieudanej próbie. Kaspersky Endpoint Security wyświetla czas blokowania dla urządzenia USB. Po upływie tego czasu możesz mieć 5 prób wprowadzenia kodu autoryzacyjnego.
Limit czasu po osiągnięciu maksymalnej liczby prób (minuty)	Czas blokowania urządzenia USB po określonej liczbie nieudanych prób wprowadzenia kodu autoryzacyjnego. Ważne wartości to 1 do 180 (minuty).

Ochrona AMSI

Komponent Ochrona AMSI jest przeznaczony do obsługi Antimalware Scan Interface firmy Microsoft. *Antimalware Scan Interface (AMSI)* umożliwia aplikacjom firm trzecich z obsługą AMSI wysyłanie obiektów (na przykład, skryptów PowerShell) do Kaspersky Endpoint Security w celu przeprowadzenia dodatkowego skanowania i otrzymania wyników ze skanowania tych obiektów. Aplikacje firm trzecich mogą obejmować, na przykład, aplikacje Microsoft Office (patrz rysunek poniżej). Więcej informacji na temat AMSI znajdziesz w [dokumentacji firmy Microsoft](#).

Ochrona AMSI może tylko wykrywać zagrożenia i informować aplikację firmy trzeciej o wykrytym zagrożeniu. Aplikacja firmy trzeciej po odebraniu powiadomienia o zagrożeniu nie zezwala na wykonanie szkodliwych działań (na przykład, kończy proces).



Przykład działania AMSI

Komponent Ochrona AMSI może odrzucić żądanie z aplikacji firmy trzeciej, na przykład, jeśli ta aplikacja przekracza maksymalną liczbę żądań w określonym przedziale czasu. Kaspersky Endpoint Security wyśle informacje o odrzuconym żądaniu z aplikacji firmy trzeciej do Serwera administracyjnego. Komponent Ochrona AMSI nie odrzuca żądań od tych aplikacji firm trzecich, dla których pole [Nie blokuj interakcji z modułem Ochrona AMSI](#) jest zaznaczone.

Ochrona AMSI jest dostępny dla następujących systemów operacyjnych dla stacji roboczych i serwerów:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise;
- Windows 11;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Ustawienia Ochrony AMSI

Parametr	Opis
Skanuj archiwa	Skanuje archiwa w następujących formatach: RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
Skanuj pakiety dystrybucyjne	To pole włącza/wyłącza skanowanie pakietów dystrybucyjnych firm trzecich.
Skanuj pliki w formatach Microsoft Office	Skanuje pliki Microsoft Office (DOC, DOCX, XLS, PPT i inne rozszerzenia Microsoft). Pliki formatu Office OLE zawierają także obiekty.
Nie rozpakowuj dużych plików złożonych	Jeżeli to pole jest zaznaczone, Kaspersky Endpoint Security nie skanuje plików złożonych, o ile ich rozmiar przekracza określoną wartość. Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security skanuje pliki złożone o wszystkich rozmiarach. Kaspersky Endpoint Security skanuje pliki o dużych rozmiarach, które zostają wypakowane z archiwów niezależnie od tego, czy pole jest zaznaczone.

Ochrona przed exploitami

Komponent Ochrona przed exploitami wykrywa kod programu, który wykorzystuje luki na komputerze, aby użyć uprawnień administratora lub wykonać szkodliwe aktywności. Na przykład, exploit może używać ataku typu buffer overflow (przepełnienie bufora). Aby to zrobić, exploit wysyła dużą ilość danych do aplikacji zawierającej lukę. Podczas przetwarzania tych danych aplikacja zawierająca lukę wykona szkodliwy kod. W wyniku tego ataku exploit może uruchomić nieautoryzowaną instalację szkodliwego programu. Po wykryciu, że próba uruchomienia pliku wykonywalnego z aplikacji zawierającej lukę nie została zainicjowana przez użytkownika, Kaspersky Endpoint Security zablokuje uruchomienie tego pliku lub poinformuje użytkownika.

Ustawienia komponentu Ochrona przed exploitami

Parametr	Opis
Po wykryciu exploita	<p>Zablokuj operację. Jeśli ta opcja jest zaznaczona, po wykryciu exploita program Kaspersky Endpoint Security blokuje działania, które exploit próbuje wykonać.</p> <p>Informuj. Jeśli ta opcja jest zaznaczona, a exploit zostanie wykryty, Kaspersky Endpoint Security nie zablokuje działań exploita, ale doda informacje o tym exploicie do listy aktywnych zagrożeń.</p>
Włącz ochronę pamięci procesów systemowych	Jeśli ten przycisk przełącznika jest ustawiony w pozycji włączenia, Kaspersky Endpoint Security zablokuje zewnętrzne procesy, które próbują uzyskać dostęp do pamięci procesów systemowych.

Wykrywanie zachowań

Komponent Wykrywanie zachowań gromadzi dane na temat działań aplikacji na komputerze i dostarcza te informacje innym składnikom ochrony w celu udoskonalenia ich działania. Komponent Wykrywanie zachowań używa sygnatur strumieni zachowań (BSS) dla aplikacji. Jeśli aktywność aplikacji odpowiada sygnaturze strumienia zachowań, Kaspersky Endpoint Security wykona wybrane działanie. Funkcjonalność Kaspersky Endpoint Security oparta na sygnaturach strumieni zachowań zapewnia ochronę proaktywną komputera.

Ustawienia komponentu Wykrywanie zachowań

Parametr	Opis
Po wykryciu aktywności szkodliwego oprogramowania	<ul style="list-style-type: none"> • Usuń plik. Jeśli ta opcja jest zaznaczona, po wykryciu szkodliwej aktywności program Kaspersky Endpoint Security usunie plik wykonywalny szkodliwej aplikacji i utworzy kopię zapasową pliku w Kopii zapasowej. • Przerwij działanie aplikacji. Jeśli ta opcja jest zaznaczona, po wykryciu szkodliwej aktywności Kaspersky Endpoint Security zakończy działanie tej aplikacji. • Informuj. Jeśli ta opcja jest zaznaczona i zostanie wykryta szkodliwa aktywność aplikacji, Kaspersky Endpoint Security nie zakończy działania tej aplikacji, ale doda informację o szkodliwej aktywności tej aplikacji do listy aktywnych zagrożeń.
Włącz ochronę folderów współdzielonych przed szyfrowaniem zewnętrznym	<p>Jeśli przycisk przełącznika jest ustawiony w pozycji włączenia, Kaspersky Endpoint Security przeanalizuje aktywność w folderach współdzielonych. Jeśli to działanie jest zgodne z sygnaturą strumieni zachowań, która jest typowa dla zewnętrznego szyfrowania, Kaspersky Endpoint Security wykonuje wybraną akcję.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Kaspersky Endpoint Security zapobiega szyfrowaniu zewnętrznemu tylko tych plików, które znajdują się na nośniku z systemem plików NTFS i nie są szyfrowane przez system EFS.</p> </div>

	<ul style="list-style-type: none"> • Informuj. Jeśli ta opcja jest zaznaczona, po wykryciu próby zmodyfikowania plików w folderach współdzielonych, Kaspersky Endpoint Security doda informacje o tej próbie zmodyfikowania plików w folderach współdzielonych do listy aktywnych zagrożeń. • Blokuj połączenie przez N min. Jeśli ta opcja jest zaznaczona, gdy Kaspersky Endpoint Security wykryje próbę zmodyfikowania plików w folderach współdzielonych, zablokuje aktywność sieciową komputera, który próbuje zmodyfikować pliki i utworzy kopie zapasowe zmodyfikowanych plików. <div data-bbox="411 434 1493 555" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Jeśli komponent Silnik korygujący jest włączony, a opcja Blokuj połączenie przez N min jest zaznaczona, zmodyfikowane pliki zostaną przywrócone z kopii zapasowych.</p> </div>
<p>Wykluczenia</p>	<p>Lista komputerów, z których próby zaszyfrowania folderów współdzielonych nie będą monitorowane.</p> <div data-bbox="411 728 1493 954" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Aby zastosować listę wykluczeń komputerów z ochrony folderów współdzielonych przed zewnętrznym szyfrowaniem, należy włączyć Przeprowadź inspekcję logowania w zasadach inspekcji zabezpieczeń Windows. Domyślnie Przeprowadź inspekcję logowania jest wyłączone. Więcej informacji o zasadach inspekcji zabezpieczeń Windows można znaleźć na stronie internetowej firmy Microsoft.</p> </div>

Ochrona przed włamaniami

Ochrona przed włamaniami uniemożliwia aplikacjom wykonywanie działań niebezpiecznych dla systemu operacyjnego i zapewnia kontrolę dostępu do zasobów systemu operacyjnego i danych osobowych. Komponent zapewnia ochronę komputera za pomocą antywirusowych baz danych, usługi w chmurze Kaspersky Security Network.

Komponent kontroluje działanie aplikacji za pomocą *uprawnień aplikacji*. Uprawnienia aplikacji obejmują następujące parametry dostępu:

- Dostęp do zasobów systemu operacyjnego (na przykład opcje automatycznego uruchamiania, klucze rejestru)
- Dostęp do danych osobowych (takich jak pliki i aplikacje)

Aktywność sieciowa aplikacji jest kontrolowana przez [Zaporę sieciową](#) za pomocą *reguł sieciowych*.

Podczas pierwszego uruchomienia aplikacji Ochrona przed włamaniami wykonuje następujące działania:

1. Sprawdza bezpieczeństwo aplikacji przy użyciu pobranych antywirusowych baz danych.
2. Sprawdza bezpieczeństwo aplikacji w Kaspersky Security Network.

Zalecane jest [uczestniczenie w Kaspersky Security Network](#), aby zapewnić bardziej efektywne działanie komponentu Ochrona przed włamaniami.

3. Umieszcza aplikację w jednej z *grup zaufania*: Zaufane, Niski poziom ograniczeń, Wysoki poziom ograniczeń, Niezaufane.

Grupa zaufania określa uprawnienia, do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.

Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania dla składników Zapora sieciowa i Ochrona przed włamaniami. Nie można zmienić grupy zaufania tylko dla Zapory sieciowej lub Ochrony przed włamaniami.

Jeśli odmówiłeś uczestnictwa w KSN lub nie ma sieci, Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od ustawień modułu Ochrona przed włamaniami. Po otrzymaniu reputacji aplikacji od KSN, grupę zaufania można zmienić automatycznie.

4. Blokuję działania aplikacji w zależności od grupy zaufania. Na przykład, aplikacje z grupy Wysoki poziom ograniczeń mają zablokowany dostęp do modułów systemu operacyjnego.

Przy następnym uruchomieniu aplikacji, Kaspersky Endpoint Security sprawdzi integralność aplikacji. Jeżeli aplikacja nie została zmieniona, moduł użyje dla niej bieżących uprawnień aplikacji. Jeżeli aplikacja została zmodyfikowana, Kaspersky Endpoint Security analizuje aplikację tak, jakby była uruchamiana po raz pierwszy.

Ustawienia komponentu Ochrona przed włamaniami

Parametr	Opis
Uprawnienia aplikacji	<p>Aplikacje</p> <p>Tabela aplikacji monitorowanych przez komponent Ochrona przed włamaniami. Aplikacje są przypisywane do grup zaufania. Grupa zaufania określa uprawnienia, do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji.</p> <p>Możesz wybrać aplikację z jednej listy wszystkich aplikacji zainstalowanych na komputerach pod kontrolą zasady i dodać aplikację do grupy zaufania.</p> <p>Prawa dostępu do aplikacji zostały przedstawione w następujących tabelach:</p> <ul style="list-style-type: none">• Pliki i rejestr systemu. Ta tabela zawiera prawa aplikacji w grupie zaufania do uzyskania dostępu do zasobów systemu operacyjnego i danych osobowych.• Uprawnienia. Ta tabela zawiera uprawnienia aplikacji w grupie zaufania w celu uzyskania dostępu do procesów i zasobów systemu operacyjnego.• Reguły sieciowe. Tabela reguł sieciowych dla aplikacji należących do grupy zaufania. Zgodnie z tymi regułami <u>Zapora sieciowa</u> reguluje aktywność sieciową aplikacji. Tabela wyświetla predefiniowane reguły sieciowe, które są zalecane przez ekspertów z Kaspersky. Te reguły sieciowe zostały dodane w celu optymalnej ochrony ruchu sieciowego komputerów z systemami operacyjnymi Windows. Nie można usunąć predefiniowanych reguł sieciowych.
Chronione zasoby	<p>Nazwa</p> <p>Tabela zawiera zasoby komputera podzielone na kategorie. Ochrona przed włamaniami monitoruje próby dostępu innych aplikacji do zasobów znajdujących się w tabeli. Zasobem może być kategoria rejestru, plik lub folder, bądź klucz rejestru.</p>

	<p>Aplikacje</p> <p>Tabela aplikacji monitorowanych przez komponent Ochrona przed włamaniami dla wybranego zasobu. Aplikacje są przypisywane do grup zaufania. Grupa zaufania określa uprawnienia, do których program Kaspersky Endpoint Security odnosi się podczas kontrolowania aktywności aplikacji.</p>
<p>Grupa zaufania dla aplikacji uruchamianych zanim Kaspersky Endpoint Security for Windows zacznie działać</p>	<p>Grupa zaufania, w której Kaspersky Endpoint Security umieści aplikacje uruchomione przed Kaspersky Endpoint Security.</p>
<p>Aktualizuj uprawnienia dla wcześniej nieznanymi aplikacji z bazy danych KSN</p>	<p>Jeśli pole jest zaznaczone, Ochrona przed włamaniami aktualizuje uprawnienia dla wcześniej nieznanymi aplikacji przy użyciu bazy danych Kaspersky Security Network.</p>
<p>Ufaj aplikacjom podpisanym cyfrowo</p>	<p>Jeśli pole jest zaznaczone, Ochrona przed włamaniami umieszcza aplikacje posiadające podpis cyfrowy zaufanych dostawców w grupie Zaufane.</p> <p><i>Zaufani producenci</i> to producenci oprogramowania, którzy zostali umieszczeni w grupie zaufania przez Kaspersky. Możesz także ręcznie dodać certyfikat producenta do magazynu zaufanych certyfikatów.</p> <p>Jeśli pole nie jest zaznaczone, Ochrona przed włamaniami nie uważa takich aplikacji za zaufane i wykorzystuje inne parametry do określenia ich grupy zaufania.</p>
<p>Usuń reguły dla aplikacji, które nie były uruchamiane dłużej niż N dni</p>	<p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security automatycznie usuwa informacje o aplikacji (grupa zaufania i uprawnienia dostępu), jeśli spełnione są następujące warunki:</p> <ul style="list-style-type: none"> • Możesz ręcznie umieścić aplikację w grupie zaufania lub skonfigurować jej uprawnienia dostępu. • Aplikacja nie została uruchomiona w określonym przedziale czasu. <p>Jeśli grupa zaufania i uprawnienia aplikacji zostały określone automatycznie, Kaspersky Endpoint Security usunie informacje o tej aplikacji po 30 dniach. Nie jest możliwa zmiana okresu przechowywania informacji o aplikacji ani wyłączenie automatycznego usuwania.</p> <p>Następnym razem, gdy uruchomisz tę aplikację, Kaspersky Endpoint Security analizuje aplikację w taki sposób, jakby była uruchamiana po raz pierwszy.</p>
<p>Grupa zaufania dla aplikacji, których nie można dodać do istniejących grup</p>	<p>Elementy na liście rozwijalnej określają, do której grupy zaufania program Kaspersky Endpoint Security przydzieli nieznaną aplikację.</p> <p>Możesz wybrać jeden z następujących elementów:</p> <ul style="list-style-type: none"> • Niskie ograniczenia. • Wysokie ograniczenia. • Niezaufane.

Silnik korygujący

Silnik korygujący umożliwia Kaspersky Endpoint Security wycofanie działań, które zostały wykonane przez szkodliwe oprogramowanie w systemie operacyjnym.

Podczas cofania szkodliwej aktywności w systemie operacyjnym Kaspersky Endpoint Security podejmuje działanie na następujących typach szkodliwej aktywności:

- **Aktywność plikowa**

Kaspersky Endpoint Security wykonuje następujące działania:

- Usuwa pliki wykonywalne, które zostały utworzone przez szkodliwe oprogramowanie (na wszystkich mediach za wyjątkiem dysków sieciowych).
- Usuwa pliki wykonywalne, które zostały utworzone przez programy, do których przeniknęło szkodliwe oprogramowanie.
- Przywraca pliki, które zostały zmodyfikowane lub usunięte przez szkodliwe oprogramowanie.

Funkcja odzyskiwania plików posiada [kilka ograniczeń](#).

- **Aktywność w rejestrze**

Kaspersky Endpoint Security wykonuje następujące działania:

- Usuwa klucze rejestru, które zostały utworzone przez szkodliwe oprogramowanie.
- Nie przywraca kluczy rejestru, które zostały zmodyfikowane lub usunięte przez szkodliwe oprogramowanie.

- **Aktywność w systemie**

Kaspersky Endpoint Security wykonuje następujące działania:

- Kończy procesy, które zostały zainicjowane przez szkodliwe oprogramowanie.
- Kończy procesy, do których przeniknęła szkodliwa aplikacja.
- Nie wznawia procesów zatrzymanych przez szkodliwy program.

- **Aktywność sieciowa**

Kaspersky Endpoint Security wykonuje następujące działania:

- Blokuję aktywność sieciową szkodliwego oprogramowania.
- Blokuję aktywność sieciową procesów, do których przeniknęło szkodliwe oprogramowanie.

Wycofanie działań szkodliwych programów może być zainicjowane przez komponent [Ochrona plików](#) lub [Wykrywanie zachowań](#) lub podczas [skanowania antywirusowego](#).

Wycofywanie działań szkodliwego oprogramowania oddziałuje na ściśle określony zestaw danych. Nie ma negatywnego wpływu na system operacyjny i integralność danych komputera.

Aby lepiej chronić Twój komputer, Kaspersky Endpoint Security wykorzystuje dane otrzymane od użytkowników z całego świata. Usługa Kaspersky Security Network została zaprojektowana do gromadzenia tych danych.

Kaspersky Security Network (KSN) jest usługą chmury oferującą dostęp do internetowej Bazy Wiedzy firmy Kaspersky, zawierającej informacje o reputacji plików, zasobów sieciowych oraz oprogramowania. Korzystanie z danych z Kaspersky Security Network zapewnia przyspieszenie czasu odpowiedzi programu Kaspersky Endpoint Security na nowe zagrożenia, ulepszenie działania niektórych modułów ochrony oraz zmniejszenie ryzyka fałszywych alarmów. Jeśli uczestniczysz w Kaspersky Security Network, usługi KSN zapewniają Kaspersky Endpoint Security informacje o kategorii i reputacji przeskanowanych plików, a także informacje o reputacji przeskanowanych adresów internetowych.

Korzystanie z Kaspersky Security Network jest dobrowolne. Aplikacja oferuje użytkownikowi możliwość korzystania z KSN podczas wstępnej konfiguracji aplikacji. Użytkownik może rozpocząć lub zakończyć uczestniczenie w KSN w dowolnym momencie.

Więcej informacji na temat wysyłania do Kaspersky informacji statystycznych, wygenerowanych w trakcie uczestnictwa w KSN, a także informacji o przechowywaniu i niszczeniu takich informacji można znaleźć w Umowie Kaspersky Security Network oraz na [stronie Kaspersky](#). Plik ksn_<ID języka>.txt zawierający treść Oświadczenia Kaspersky Security Network znajduje się w [pakiecie dystrybucyjnym](#) aplikacji.

Aby zmniejszyć obciążenie na serwerach KSN, eksperci z Kaspersky mogą opublikować aktualizacje aplikacji, które tymczasowo wyłączą lub częściowo ograniczą żądania do Kaspersky Security Network. W tym przypadku stan połączenia z KSN w lokalnym interfejsie aplikacji jest *Włączony z ograniczeniami*.

Infrastruktura KSN

Kaspersky Endpoint Security obsługuje następujące rozwiązania infrastrukturalne KSN:

- *Globalna sieć KSN* to rozwiązanie używane przez większość aplikacji Kaspersky. Uczestnicy KSN otrzymują informacje z Kaspersky Security Network i wysyłają do Kaspersky informacje o obiektach wykrytych na komputerze użytkownika w celu dodatkowego przeanalizowania przez analityków Kaspersky i znajdujących się w bazach danych reputacji oraz statystycznych bazach danych usługi Kaspersky Security Network.
- *Prywatna sieć KSN* to rozwiązanie, które umożliwia użytkownikom komputerów z zainstalowanym programem Kaspersky Endpoint Security lub innymi aplikacjami Kaspersky uzyskanie dostępu do baz danych reputacji Kaspersky Security Network oraz innych danych statystycznych bez wysyłania danych do KSN z ich własnych komputerów. Prywatna sieć KSN została zaprojektowana dla klientów korporacyjnych, którzy nie mogą uczestniczyć w Kaspersky Security Network z dowolnego z następujących powodów:
 - Lokalne stacje robocze nie są połączone z internetem.
 - Przesyłanie wszelkich danych poza kraj lub poza korporacyjną sieć LAN są zabronione przez prawo lub ograniczone przez politykę bezpieczeństwa firmy.

Domyślnie Kaspersky Security Center używa Global KSN. Możesz skonfigurować użycie Prywatnej sieci KSN w Konsoli administracyjnej (MMC) i Kaspersky Security Center Web Console oraz w [wierszu polecenia](#). Nie można skonfigurować korzystania z Prywatnej sieci KSN w konsoli Kaspersky Security Center Cloud Console.

Więcej informacji o Prywatnej sieci KSN można znaleźć w *dokumentacji do Kaspersky Private Security Network*.

KSN Proxy

Komputery użytkowników zarządzane przez Kaspersky Security Center Administration Server mogą komunikować się z KSN poprzez usługę KSN Proxy.

Usługa KSN Proxy posiada następujące możliwości:

- Komputer użytkownika może łatwo odpytywać KSN i przysyłać informacje do KSN, nawet bez bezpośredniego dostępu do internetu.
- Usługa KSN Proxy buforuje przetwarzane dane, ograniczając obciążenie zewnętrznego kanału komunikacji sieciowej i przyspieszając odbieranie informacji żądanych przez komputer użytkownika.

Więcej informacji na temat usługi KSN Proxy można znaleźć w [pomocy do Kaspersky Security Center](#).

Ustawienia Kaspersky Security Network

Parametr	Opis
Włącz rozszerzony tryb KSN	<i>Rozszerzony tryb KSN</i> to tryb, w którym Kaspersky Endpoint Security wysyła dodatkowe dane do Kaspersky. Kaspersky Endpoint Security używa KSN do wykrywania zagrożeń niezależnie od pozycji przełącznika.
Włącz tryb chmury	<p><i>Tryb chmury</i> odnosi się do trybu działania aplikacji, w którym Kaspersky Endpoint Security używa lekkiej wersji antywirusowych baz danych. Kaspersky Security Network obsługuje działanie aplikacji, gdy używana jest lekka wersja antywirusowych baz danych. Lekka wersja antywirusowych baz danych umożliwia korzystanie z około połowy pamięci RAM komputera, która inaczej zostałaby użyta ze zwykłymi bazami danych. Jeśli nie uczestniczysz w Kaspersky Security Network lub jeśli tryb chmury jest wyłączony, Kaspersky Endpoint Security pobierze pełną wersję antywirusowych baz danych z serwerów Kaspersky.</p> <p>Jeśli przycisk przełącznika jest ustawiony w pozycji włączenia, Kaspersky Endpoint Security używa podstawowej wersji antywirusowych baz danych, co zmniejsza zużycie zasobów systemu operacyjnego.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Po zaznaczeniu pola, Kaspersky Endpoint Security pobierze podstawową wersję antywirusowych baz danych podczas kolejnej aktualizacji.</p> </div> <p>Jeśli przycisk przełącznika jest ustawiony w pozycji wyłączenia, Kaspersky Endpoint Security używa kompletnej wersji antywirusowych baz danych.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Po odznaczeniu pola, Kaspersky Endpoint Security pobierze kompletną wersję antywirusowych baz danych podczas kolejnej aktualizacji.</p> </div>
Stan komputera, gdy serwery KSN są niedostępne <i>(dostępny tylko w Kaspersky Security Center Console)</i>	Elementy na liście rozwijalnej określają stan komputera w Kaspersky Security Center, gdy serwery KSN są niedostępne.
Użyj KSN Proxy	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security używa usługi KSN Proxy. Możliwe jest skonfigurowanie ustawień usługi KSN Proxy we właściwościach Serwera

(dostępny tylko w Kaspersky Security Center Console)	administracyjnego.
Użyj serwerów KSN, jeżeli KSN Proxy jest niedostępny (dostępny tylko w Kaspersky Security Center Console)	Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security używa serwerów KSN, jeśli usługa KSN Proxy jest niedostępna. Serwery KSN mogą znajdować się po stronie Kaspersky (gdy używana jest usługa Globalna sieć KSN) oraz po stronie stron trzecich (gdy używana jest usługa Prywatna sieć KSN).

Kontrola sieci

Kontrola sieci zarządza dostępem użytkowników zasobów sieciowych. Pomaga to zmniejszyć ruch sieciowy i nieodpowiednie dysponowanie czasem pracy. Gdy użytkownik próbuje otworzyć stronę internetową ograniczoną przez Kontrolę sieci, Kaspersky Endpoint Security zablokuje dostęp lub wyświetli ostrzeżenie (patrz rysunek poniżej).

Kaspersky Endpoint Security monitoruje tylko ruch HTTP i HTTPS.

Dla monitorowania ruchu HTTPS należy [włączyć skanowanie zaszyfrowanych połączeń](#).

Metody zarządzania dostępem do stron internetowych

Kontrola sieci umożliwia konfigurowanie dostępu do stron internetowych przy użyciu następujących metod:

- **Kategoria strony internetowej.** Strony internetowe są kategoryzowane zgodnie z usługą chmury Kaspersky Security Network, analizą heurystyczną i bazą danych znanych stron internetowych (znajdącą się w bazach danych aplikacji). Na przykład, możesz ograniczyć dostęp użytkownika do kategorii „Sieci społecznościowe” lub do [innych kategorii](#).
- **Typ danych.** Na przykład, możesz ograniczyć dostęp użytkowników do danych na stronie internetowej i ukryć zawartość graficzną. Kaspersky Endpoint Security określa typ danych w oparciu o format pliku, a nie w oparciu o jego rozszerzenie.

Kaspersky Endpoint Security nie skanuje plików w archiwach. Na przykład, jeśli pliki obrazów zostały umieszczone w archiwum, Kaspersky Endpoint Security identyfikuje typ danych „Archiwa”, a nie „Pliki graficzne”.

- **Określony adres.** Możesz wprowadzić adres internetowy lub [użyć masek](#).

Możesz jednocześnie użyć kilku metod do regulowania dostępu do stron internetowych. Na przykład, możesz ograniczyć dostęp do typu danych „Pliki biurowe” tylko dla kategorii stron internetowych „Poczta przez WWW”.

Reguły dostępu do stron internetowych

Kontrola sieci zarządza dostępem użytkowników do stron internetowych przy użyciu *reguł dostępu*. Możesz skonfigurować następujące zaawansowane ustawienia reguły dostępu do stron internetowych:

- Użytkowników, do których stosowana jest reguła.

Na przykład, możesz ograniczyć dostęp do internetu poprzez przeglądarkę dla wszystkich użytkowników firmy, za wyjątkiem działu IT.

- Terminarz reguły.

Na przykład, możesz ograniczyć dostęp do internetu poprzez przeglądarkę tylko w trakcie godzin pracy.

Priorytety reguł dostępu

Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli strona internetowa została dodana do kilku reguł, Kontrola sieci reguluje dostęp do strony internetowej w oparciu o regułę z najwyższym priorytetem. Na przykład, Kaspersky Endpoint Security może identyfikować portal firmowy jako sieć społecznościową. Aby ograniczyć dostęp do sieci społecznościowych i zapewnić dostęp do firmowego portalu internetowego, utwórz dwie reguły: jedną regułę blokady dla kategorii stron internetowych „Sieci społecznościowe” i jedną regułę zezwalającą dla firmowego portalu internetowego. Reguła dostępu dla firmowego portalu internetowego musi posiadać wyższy priorytet niż reguła dostępu dla sieci społecznościowych.



Żądana strona internetowa nie może zostać wyświetlona.

Adres: <http://kaspersky.ru/>.

Strona internetowa została zablokowana zgodnie z regułą block.

Powód: zasób sieciowy należy do kategorii zawartości Nieokreślony i kategorii rodzaju danych Nieokreślony.

Ten zasób sieciowy jest zabroniony w firmie. Jeżeli uważasz, że zasób sieciowy został niesłusznie zablokowany lub potrzebujesz do niego dostęp, skontaktuj się z administratorem firmowej sieci lokalnej ([Poproś o dostęp](#)).

Komunikat wygenerowano: 10/29/2020 3:45:02 AM



Żądana strona może być niebezpieczna lub zabroniona przez politykę firmy.

Adres: <http://www.kaspersky.com/>.

Strona internetowa została zablokowana zgodnie z regułą warn.

Powód: zasób sieciowy należy do kategorii zawartości: Nieokreślony i kategorii rodzaju danych: Nieokreślony.

Kliknij odsyłacz <http://www.kaspersky.com/>, aby otworzyć tę stronę.

Aby uzyskać dostęp do całej zawartości strony, kliknij odsyłacz <http://www.kaspersky.com/>.

Aby uzyskać dostęp do wszystkich istniejących domen należących do tego samego lub niższego poziomu z tą oznaczoną gwiazdką "*", kliknij odsyłacz [*://*.kaspersky.com/](http://*.kaspersky.com/).

Dostęp do wymienionych powyżej zasobów sieciowych zostanie przydzielony na czas trwania obecnej sesji Kaspersky Endpoint Security.

W przypadku pomyłkowego ostrzeżenia, skontaktuj się z administratorem firmowej sieci lokalnej ([Poproś o dostęp](#)).

Komunikat wygenerowano: 10/29/2020 3:44:55 AM

Wiadomości Kontroli sieci

Ustawienia komponentu Kontrola sieci

Parametr	Opis
Reguły dostępu do zasobów sieciowych	Lista zawierająca reguły dostępu do zasobu sieciowego. Każda reguła posiada priorytet. Im wyżej reguła znajduje się na liście reguł, tym wyższy priorytet posiada. Jeśli strona internetowa została dodana do kilku reguł, Kontrola sieci reguluje dostęp do strony internetowej w oparciu o regułę z najwyższym priorytetem.
Reguła domyślna	<i>Domyślna reguła</i> to reguła dostępu do zasobów internetowych, które nie są objęte żadną inną regułą. Dostępne są następujące opcje: <ul style="list-style-type: none">• Zezwól na wszystko poza listą reguł, także znana jako tryb listy zablokowanych dla zabronionych stron internetowych.• Odrzuć wszystko poza listą reguł, także znana jako tryb listy zezwolonych dla dozwolonych stron internetowych.
Szablony wiadomości	<ul style="list-style-type: none">• Ostrzeżenie. Pole do wprowadzenia danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła ostrzegająca o próbach uzyskania dostępu do niechcianych zasobów sieciowych.

	<ul style="list-style-type: none"> • Wiadomość dotycząca blokowania. To pole do wprowadzania danych zawiera szablon wiadomości wyświetlanej, gdy zostaje wyzwolona reguła blokująca dostęp do zasobu sieciowego. • Wiadomość do administratora. Szablon wiadomości wysyłanej do administratora sieci LAN, gdy użytkownik uważa blokadę za pomyłkę. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: Wiadomość do administratora dotycząca zablokowania dostępu do strony internetowej Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń Żądania użytkowników. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.
<p>Zapisuj informacje o otwarciu dozwolonych stron</p>	<p>Kaspersky Endpoint Security zapisuje dane dotyczące odwiedzin na wszystkich stronach internetowych, w tym dozwolonych stronach internetowych. Kaspersky Endpoint Security wysyła zdarzenia do Kaspersky Security Center, do lokalnego raportu Kaspersky Endpoint Security, a także do dziennika zdarzeń systemu Windows. Aby monitorować aktywność internetową użytkownika, należy skonfigurować ustawienia zapisywania zdarzeń.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Monitorowanie aktywności użytkownika w internecie może wymagać więcej zasobów komputera podczas deszyfrowania ruchu HTTPS.</p> </div>

Kontrola urządzeń

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Kontrola urządzeń zarządza dostępem użytkownika do urządzeń, które są instalowane na komputerze lub są podłączone do komputera (na przykład: dyski twarde, kamery lub moduły Wi-Fi). Umożliwia to ochronę komputera przed infekcją, gdy takie urządzenia są podłączone, oraz zapobieganie utracie lub wyciekowi danych.

Poziomy dostęp do urządzenia

Kontrola urządzeń kontroluje dostęp na następujących poziomach:

- **Typ urządzenia.** Na przykład: drukarki, dyski wymienne oraz płyty CD/DVD.

Dostęp urządzenia możesz skonfigurować w następujący sposób:

- Zezwól – ✓.
- Zablokuj – ⓧ.
- Zależy od magistrali połączeń (za wyjątkiem Wi-Fi) – 🌐.
- Blokuj z wyjątkami (tylko Wi-Fi) – 📶.

- **Magistrala połączeń.** *Magistrala połączeń* to interfejs używany do podłączania urządzeń do komputera (na przykład: USB lub FireWire). Dlatego możesz ograniczyć podłączenie wszystkich urządzeń, na przykład, za pośrednictwem USB.

Dostęp urządzenia możesz skonfigurować w następujący sposób:

- Zezwól – ✓.
 - Zablokuj – ❌.
- **Zaufane urządzenia.** *Zaufane urządzenia* są urządzeniami, do których użytkownicy, określone w ustawieniach zaufanego urządzenia, mają przez cały czas pełne prawa dostępu.

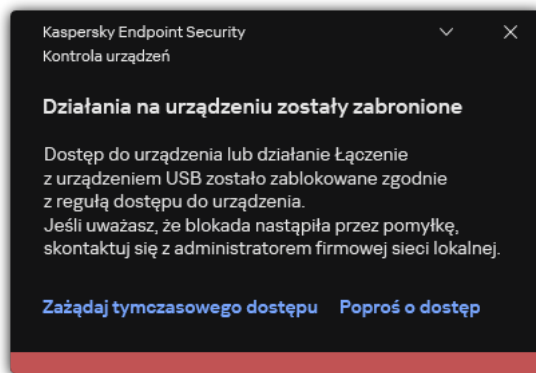
Możesz dodać zaufane urządzenia w oparciu o następujące dane:

- **Urządzenia według ID.** Każde urządzenie posiada unikatowy identyfikator (identyfikator sprzętu lub HWID). Możesz sprawdzić identyfikator we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Przykładowy identyfikator urządzenia: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Dodawanie urządzeń według identyfikatora jest wygodne, jeśli chcesz dodać kilka określonych urządzeń.
- **Urządzenia według modelu.** Każde urządzenie posiada identyfikator producenta (VID) oraz identyfikator produktu (PID). Możesz sprawdzić identyfikatory we właściwościach urządzenia, korzystając z narzędzi systemu operacyjnego. Szablon do wprowadzenia VID i PID: `VID_1234&PID_5678`. Dodawanie urządzeń według modelu jest wygodne, jeśli w swojej organizacji używasz urządzeń pewnego modelu. W ten sposób możesz dodać wszystkie urządzenia tego modelu.
- **Urządzenia według maski ID.** Jeśli używasz kilku urządzeń z podobnymi identyfikatorami, możesz dodać urządzenia do listy zaufanych, korzystając z maski. Znak * zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku ? podczas wprowadzania maski. Na przykład: `WDC_C*`.
- **Urządzenia według maski modelu.** Jeśli używasz kilku urządzeń z podobnymi numerami VID lub PID (na przykład, urządzeń od tego samego producenta), możesz dodać urządzenia do listy zaufanych przy użyciu masek. Znak * zastępuje dowolny zestaw znaków. Kaspersky Endpoint Security nie obsługuje znaku ? podczas wprowadzania maski. Na przykład: `VID_05AC & PID_*`.

Kontrola urządzeń reguluje dostęp użytkownika do urządzeń przy użyciu [reguł dostępu](#). Kontrola urządzeń umożliwia także zapisywanie zdarzeń podłączenia/odłączenia urządzenia. Aby zapisać zdarzenia, musisz skonfigurować rejestrację zdarzeń w profilu.

Jeśli dostęp do urządzenia zależy od magistrali połączenia (stan 🌈), Kaspersky Endpoint Security nie zapisuje zdarzeń podłączenia/odłączenia urządzenia. Aby umożliwić Kaspersky Endpoint Security zapisywanie zdarzeń podłączenia/odłączenia urządzenia, zezwól na dostęp do odpowiedniego typu urządzenia (stan ✓) lub dodaj urządzenie do listy zaufanych.

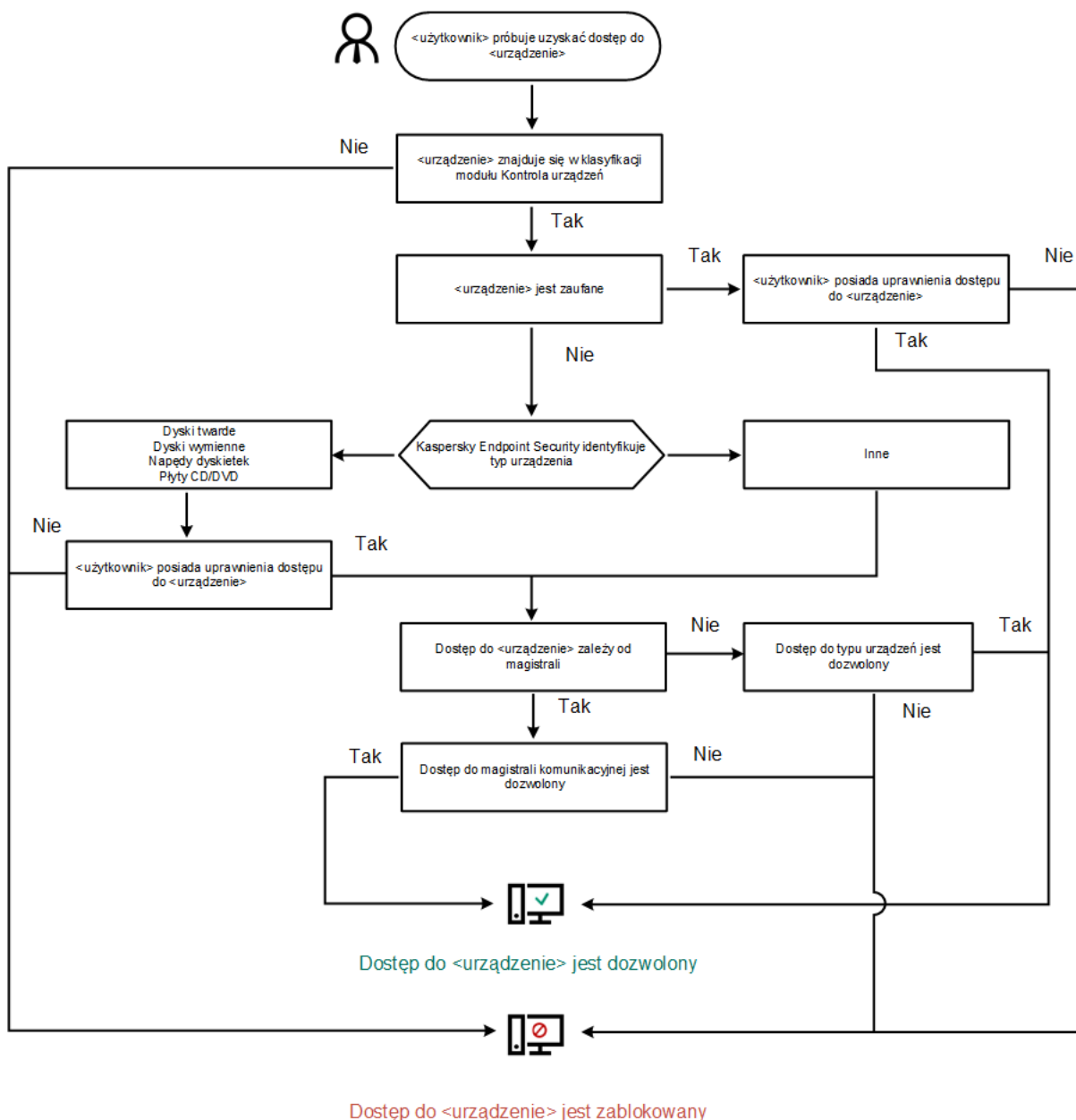
Jeśli urządzenie, które jest zablokowane przez Kontrolę urządzeń, zostanie podłączone do komputera, Kaspersky Endpoint Security zablokuje dostęp i wyświetli komunikat (patrz rysunek poniżej).



Komunikat Kontroli urządzeń

Algorytm działania Kontroli urządzeń

Kaspersky Endpoint Security podejmuje decyzję dotyczącą zezwolenia na dostęp do urządzenia po podłączeniu urządzenia do komputera przez użytkownika (patrz rysunek poniżej).



Algorytm działania Kontroli urządzeń

Jeśli urządzenie jest podłączone i dostęp jest dozwolony, możesz edytować regułę dostępu i zablokować dostęp. W tym przypadku, kolejnym razem, gdy ktoś spróbuje uzyskać dostęp do urządzenia (np. przejrzeć drzewo folderów lub wykonać operacje odczytu lub zapisu), Kaspersky Endpoint Security zablokuje dostęp. Urządzenie bez systemu plików jest blokowane dopiero przy następnym podłączeniu.

Jeśli użytkownik komputera, na którym jest zainstalowany program Kaspersky Endpoint Security, poprosi o dostęp do urządzenia, które uważa, że zostało zablokowane przez pomyłkę, wyślij do użytkownika [instrukcje wysyłania pliku żądania dostępu](#).

Ustawienia komponentu Kontrola urządzeń

Parametr	Opis
Zezwól na żądania dostępu tymczasowego <i>(dostępny tylko w Kaspersky Security Center Console)</i>	<p>Jeśli pole jest zaznaczone, przycisk Poproś o dostęp staje się dostępny poprzez lokalny interfejs Kaspersky Endpoint Security. Kliknięcie tego przycisku otwiera okno Żądanie dostępu do urządzenia. W tym oknie użytkownik może poprosić o tymczasowy dostęp do zablokowanego urządzenia.</p>
Urządzenia i sieci Wi-Fi	Ta tabela zawiera wszystkie możliwe typy urządzeń, zgodnie z klasyfikacją modułu Kontrola urządzeń, uwzględniając ich odpowiednie stany dostępu.
Magistrale połączeń	Lista wszystkich dostępnych magistrali połączeń zgodnie z klasyfikacją modułu Kontrola urządzeń, uwzględniając ich stany dostępu.
Zaufane urządzenia	Lista zaufanych urządzeń i użytkowników, którym udzielono dostępu do tych urządzeń.
Anti-Bridging	<p>Anti-Bridging zapobiega tworzeniu mostków sieciowych poprzez uniemożliwienie jednoczesnego nawiązania kilku połączeń sieciowych dla komputera. To umożliwia ochronę sieci firmowej przed atakami na niechronione, nieautoryzowane sieci.</p> <p>Anti-Bridging blokuje nawiązanie kilku połączeń zgodnie z priorytetami urządzeń. Im wyżej urządzenie znajduje się na liście, tym wyższy priorytet posiada.</p> <p>Jeśli aktywne połączenie i nowe połączenie są tego samego typu (np. Wi-Fi), Kaspersky Endpoint Security zablokuje aktywne połączenie i zezwoli na nawiązanie nowego połączenia.</p> <p>Jeśli aktywne połączenie i nowe połączenie są różnych typów (na przykład, karta sieciowa i Wi-Fi), Kaspersky Endpoint Security zablokuje połączenie z niższym priorytetem i zezwoli na połączenie z wyższym priorytetem.</p> <p>Anti-Bridging obsługuje działanie na następujących typach urządzeń: karta sieciowa, Wi-Fi i modem.</p>
Szablony wiadomości	<ul style="list-style-type: none"> • Wiadomość dotycząca blokowania. Szablon wiadomości, która pojawia się, gdy użytkownik próbuje uzyskać dostęp do zablokowanego urządzenia. Ta wiadomość pojawia się, gdy użytkownik próbuje wykonać działanie na zawartości urządzenia, które zostało zablokowane dla tego użytkownika. • Wiadomość do administratora. Szablon wiadomości, która jest wysyłana do administratora sieci LAN, gdy użytkownik uważa, że dostęp do urządzenia lub wykonywanie działań na zawartości urządzenia zostały zablokowane przez przypadek. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle

zdarzenie do Kaspersky Security Center: **Wiadomość do administratora dotycząca zablokowania dostępu do urządzenia** Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń **Żądania użytkowników**. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

Kontrola aplikacji

Kontrola aplikacji zarządza uruchamianiem aplikacji na komputerach użytkowników. Pozwala to na wdrożenie polityki bezpieczeństwa firmy podczas korzystania z aplikacji. Kontrola aplikacji zmniejsza także ryzyko infekcji komputera poprzez ograniczenie dostępu do aplikacji.

Konfiguracja Kontroli aplikacji obejmuje następujące kroki:

1. Tworzenia kategorii aplikacji.

Administrator tworzy kategorie aplikacji, którymi chce zarządzać. Kategorie aplikacji są przeznaczone dla wszystkich komputerów w sieci firmowej, niezależnie od grup administracyjnych. Do utworzenia kategorii możesz użyć następujących kryteriów: kategoria KL (na przykład, *Przeglądarki*), suma kontrolna plików, producent aplikacji i inne kryteria.

2. Tworzenie reguł Kontroli aplikacji.

Administrator tworzy reguły Kontroli aplikacji w zasadzie dla grupy administracyjnej. Reguła obejmuje kategorie aplikacji i stan uruchamiania aplikacji z tych kategorii: zablokowane lub dozwolone.

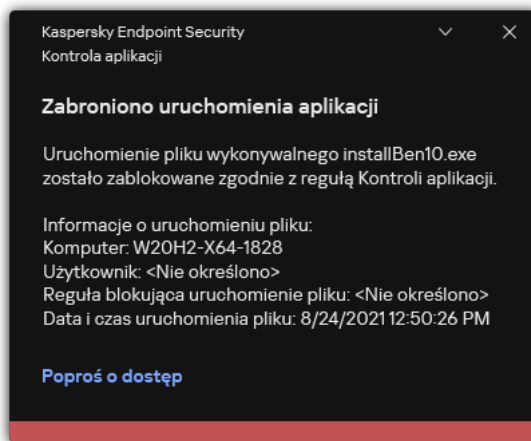
3. Wybieranie trybu Kontroli aplikacji.

Administrator wybiera tryb pracy z aplikacjami, które nie są uwzględnione w żadnej z reguł (lista zablokowanych i lista zezwolonych).

Jeśli użytkownik spróbuje uruchomić niedozwoloną aplikację, Kaspersky Endpoint Security zablokuje uruchomienie aplikacji i wyświetli powiadomienie (patrz rysunek poniżej).

Tryb testowy służy do sprawdzania konfiguracji Kontroli aplikacji. W tym trybie Kaspersky Endpoint Security wykonuje następujące czynności:

- Umożliwia uruchamianie aplikacji, w tym zabronionych.
- Wyświetla powiadomienie o uruchomieniu zabronionej aplikacji i dodaje informacje do raportu na komputerze użytkownika.
- Wysyła dane o uruchomieniu zabronionych aplikacji do Kaspersky Security Center.



Powiadomienie Kontroli aplikacji

Tryby działania Kontroli aplikacji

Komponent Kontrola aplikacji działa w dwóch trybach:

- **Lista zablokowanych.** W tym trybie Kontrola aplikacji umożliwia użytkownikom uruchamianie wszystkich aplikacji, za wyjątkiem aplikacji zabronionych w regułach Kontroli aplikacji.

Ten tryb jest włączony domyślnie.

- **Lista zezwolonych.** W tym trybie Kontrola aplikacji blokuje użytkownikom możliwość uruchamiania dowolnych aplikacji, za wyjątkiem aplikacji, które są dozwolone i nie są zabronione w regułach Kontroli aplikacji.

Jeżeli reguły zezwalające Kontroli aplikacji zostaną w pełni skonfigurowane, moduł zablokuje uruchamianie wszystkich nowych aplikacji, które nie zostały zweryfikowane przez administratora sieci LAN, natomiast zezwoli na działanie systemu operacyjnego i zaufanych aplikacji potrzebnych użytkownikom w ich pracy.

Możesz przeczytać [zalecenia odnośnie konfiguracji reguł Kontroli aplikacji w trybie listy zezwolonych](#).

Moduł Kontrola aplikacji można skonfigurować do pracy w tych trybach, korzystając z lokalnego interfejsu Kaspersky Endpoint Security oraz programu Kaspersky Security Center.

Jednakże Kaspersky Security Center oferuje narzędzia, które nie są dostępne w lokalnym interfejsie Kaspersky Endpoint Security, a które są potrzebne do:

- [Tworzenia kategorii aplikacji](#).

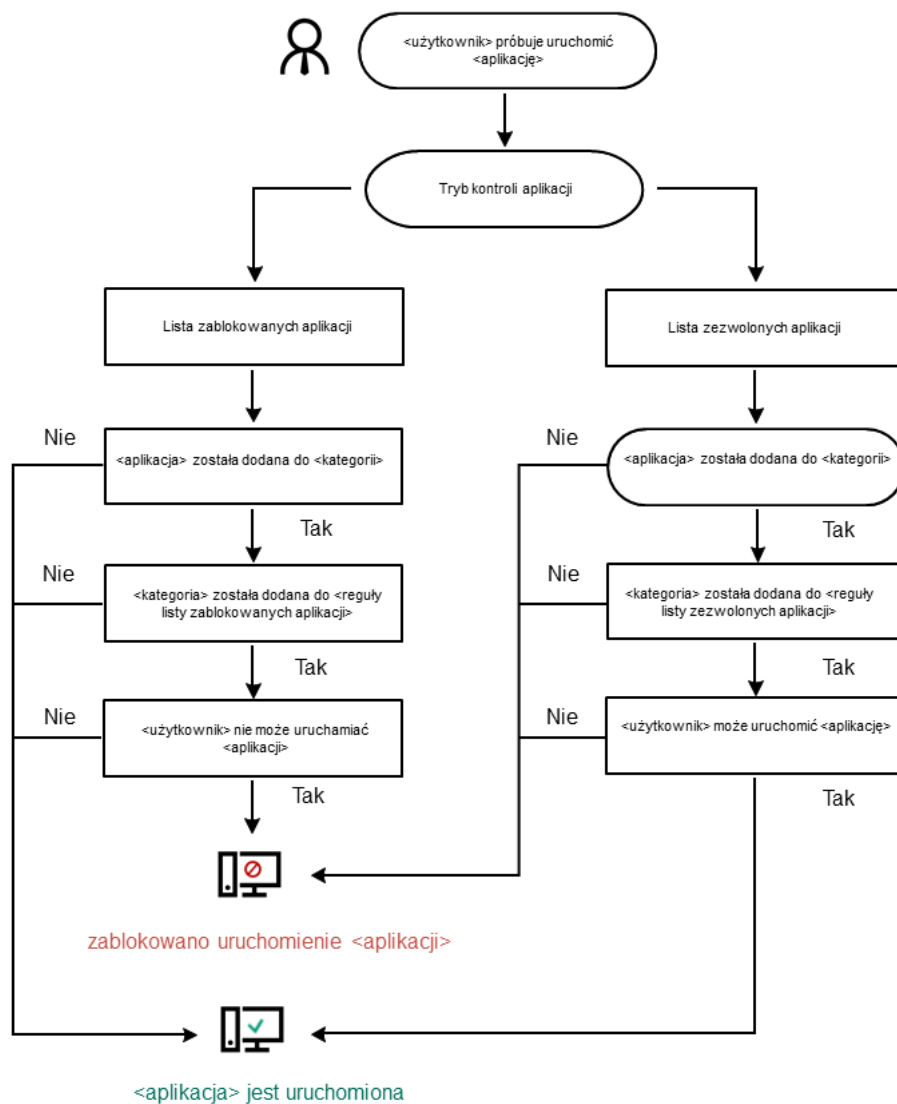
Reguły Kontroli aplikacji utworzone w Konsoli administracyjnej Kaspersky Security Center są oparte o niestandardowe kategorie aplikacji, a nie o warunki włączenia i wykluczenia, jak ma to miejsce w przypadku lokalnego interfejsu Kaspersky Endpoint Security.

- [Otrzymywania informacji o aplikacjach zainstalowanych na komputerach w korporacyjnej sieci LAN](#).

Dlatego zalecane jest korzystanie z Kaspersky Security Center podczas konfigurowania działania modułu Kontrola aplikacji.

Algorytm działania Kontroli aplikacji

Kaspersky Endpoint Security wykorzystuje algorytm do podjęcia decyzji o uruchomieniu aplikacji (patrz rysunek poniżej).



Algorytm działania Kontroli aplikacji

Ustawienia komponentu Kontrola aplikacji

Parametr	Opis
Tryb testowy	Jeśli przełącznik jest ustawiony w pozycji włączenia, Kaspersky Endpoint Security zezwala na uruchomienie aplikacji, która jest blokowana w bieżącym trybie Kontroli aplikacji, ale zapisuje informacje o jej uruchomieniu w raporcie.
Tryb Kontroli uruchamiania aplikacji	<p>Możesz wybrać jedną z następujących opcji:</p> <ul style="list-style-type: none"> Lista zablokowanych. Jeśli ta opcja jest zaznaczona, Kontrola aplikacji zezwala wszystkim użytkownikom na uruchomienie dowolnej aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł blokowania Kontroli aplikacji. Lista zezwolonych. Jeśli ta opcja jest zaznaczona, Kontrola aplikacji blokuje wszystkim użytkownikom możliwość uruchomienia jakiegokolwiek aplikacji, za wyjątkiem przypadków, gdy aplikacje spełniają warunki reguł zezwalających Kontroli aplikacji. <p>Jeśli wybrany jest tryb Lista zezwolonych, automatycznie tworzone są dwie reguły Kontroli aplikacji:</p> <ul style="list-style-type: none"> Obraz systemu.

	<ul style="list-style-type: none"> • Zaufane programy aktualizujące. <div data-bbox="367 152 1493 273" style="border: 1px solid #ccc; padding: 5px;"> <p>Nie możesz zmodyfikować ustawień ani usunąć automatycznie utworzonych reguł. Możesz włączyć lub wyłączyć te reguły.</p> </div>
<p>Kontroluj ładowanie modułów DLL</p>	<p>Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security kontroluje wczytywanie modułów DLL, gdy użytkownicy próbują uruchomić aplikacje. Informacja na temat modułu DLL i aplikacji, która załadowała ten moduł DLL, jest zapisywana w raporcie.</p> <div data-bbox="367 497 1493 792" style="border: 1px solid #ccc; padding: 5px; background-color: #f8d7da;"> <p>Po włączeniu funkcji kontrolowania wczytywania modułów DLL i sterowników, upewnij się, że w ustawieniach Kontroli aplikacji włączona jest jedna z następujących reguł: domyślna reguła Obraz systemu lub inna reguła, która zawiera kategorię KL „Zaufane certyfikaty” i zapewnia, że moduły DLL i sterowniki są ładowane przed uruchomieniem Kaspersky Endpoint Security. Włączanie kontroli ładowania modułów DLL i sterowników, gdy reguła Obraz systemu jest wyłączona, może spowodować niestabilność systemu operacyjnego.</p> </div> <p>Kaspersky Endpoint Security monitoruje tylko moduły DLL i sterowniki ładowane po zaznaczeniu pola. Po zaznaczeniu pola zalecane jest ponowne uruchomienie komputera w celu zapewnienia, że aplikacja monitoruje wszystkie sterowniki i moduły DLL, w tym te załadowane przed uruchomieniem Kaspersky Endpoint Security.</p>
<p>Szablony wiadomości</p>	<p>Wiadomość dotycząca blokowania. Szablon wiadomości wyświetlanej, gdy zostaje wywołana reguła Kontroli aplikacji, która blokuje uruchamianie aplikacji.</p> <p>Wiadomość do administratora. Szablon wiadomości, którą użytkownik może wysłać do administratora korporacyjnej sieci LAN, jeśli uważa, że aplikacja została przypadkowo zablokowana. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: Wiadomość do administratora dotycząca zablokowania uruchomienia aplikacji Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń Żądania użytkowników. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.</p>

Adaptacyjna kontrola anomalii

Ten komponent jest dostępny tylko dla Kaspersky Endpoint Security for Business Advanced i Kaspersky Total Security for Business. Więcej informacji o Kaspersky Endpoint Security for Business można znaleźć na [stronie internetowej firmy Kaspersky](#).

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Komponent Adaptacyjna kontrola anomalii monitoruje i blokuje działania, które nie są typowe dla komputerów w sieci firmowej. Adaptacyjna kontrola anomalii wykorzystuje zestaw reguł do śledzenia nietypowych zachowań (na przykład, reguła *Uruchom Microsoft PowerShell z aplikacji biurowych*). Reguły są tworzone przez specjalistów z Kaspersky w oparciu o typowe scenariusze złośliwej aktywności. Można skonfigurować, w jaki sposób Adaptacyjna kontrola aplikacji obsługuje każdą regułę i, na przykład, zezwolić na wykonywanie skryptów PowerShell, które automatyzują określone zadania przepływu pracy. Kaspersky Endpoint Security aktualizuje zestaw reguł wraz z bazami danych aplikacji. Aktualizacje zestawów reguł muszą być [potwierdzone ręcznie](#).

Ustawienia komponentu Adaptacyjna kontrola anomalii

Konfiguracja Adaptacyjnej kontroli anomalii składa się z następujących kroków:

1. Uczenie modułu Adaptacyjna kontrola anomalii.

Po włączeniu Adaptacyjnej kontroli anomalii, jej reguły działają w *trybie uczenia*. Podczas uczenia moduł Adaptacyjna kontrola anomalii monitoruje wyzwalanie reguł i wysyła zdarzenia wyzwalające do Kaspersky Security Center. Każda reguła ma swój czas trwania trybu uczenia. Czas trwania trybu uczenia jest ustawiany przez ekspertów z Kaspersky. Zazwyczaj tryb uczenia jest aktywny przez dwa tygodnie.

Jeśli podczas treningu reguła nie została w ogóle uruchomiona, Adaptacyjna kontrola anomalii uzna działania związane z tą regułą za nietypowe. Kaspersky Endpoint Security zablokuje wszystkie działania związane z tą regułą.

Jeśli reguła została wyzwolona podczas treningu, Kaspersky Endpoint Security rejestruje zdarzenia w [raporcie wyzwalającym regułę](#) oraz w repozytorium **Wywoływanie reguł w trybie Inteligentne uczenie się**.

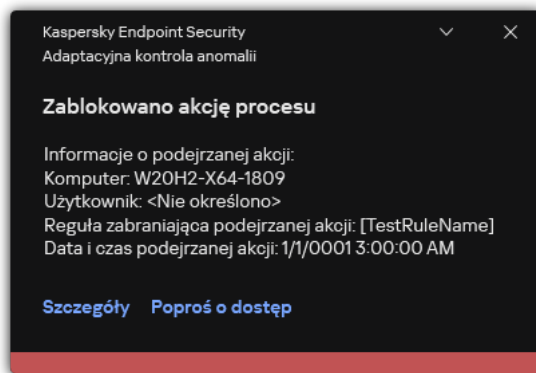
2. Analizowanie raportu dotyczącego wyzwalania reguły.

Administrator analizuje [raport dotyczący wyzwalania reguły](#) lub zawartość repozytorium **Wywoływanie reguł w trybie Inteligentne uczenie się**. Następnie administrator może wybrać zachowanie Adaptacyjnej kontroli anomalii, gdy reguła jest wyzwalana: albo zablokować, albo zezwolić. Administrator może również kontynuować monitorowanie działania reguły i wydłużyć czas trwania trybu uczenia. Jeśli administrator nie podejmie żadnych działań, aplikacja będzie również kontynuować pracę w trybie uczenia. Czas trwania trybu uczenia zostanie zrestartowany.

Adaptacyjna kontrola anomalii jest konfigurowana w czasie rzeczywistym. Adaptacyjna kontrola anomalii jest konfigurowana poprzez następujące kanały:

- Adaptacyjna kontrola anomalii automatycznie rozpoczyna blokowanie działań związanych z regułami, które nigdy nie zostały wyzwolone w trybie uczenia.
- Kaspersky Endpoint Security dodaje nowe reguły lub usuwa przestarzałe.
- Administrator konfiguruje działanie Adaptacyjnej kontroli anomalii po przejrzaniu raportu dotyczącego wyzwalania reguły i zawartości repozytorium **Wywoływanie reguł w trybie Inteligentne uczenie się**. Zalecane jest sprawdzenie raportu dotyczącego wyzwalania reguły i zawartości repozytorium **Wywoływanie reguł w trybie Inteligentne uczenie się**.

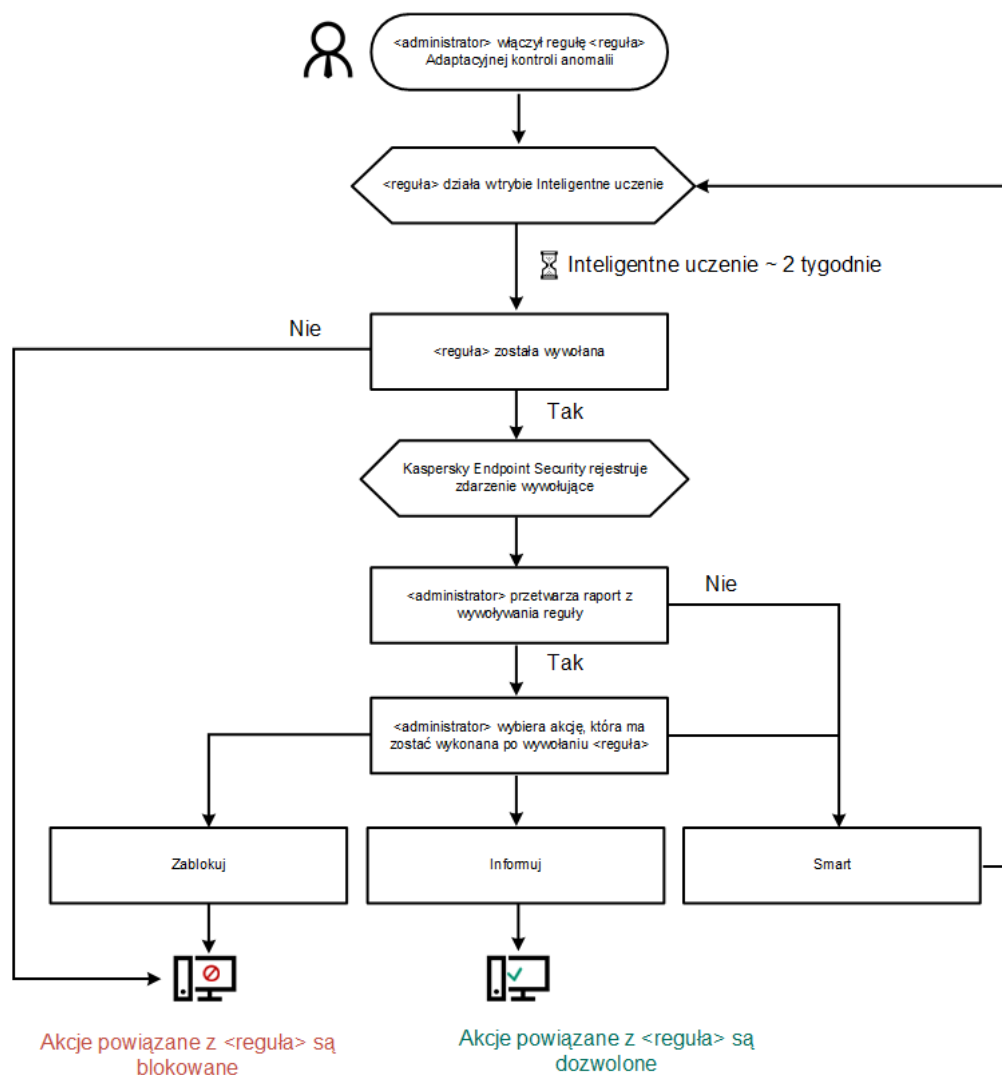
Jeśli złośliwa aplikacja spróbuje wykonać akcję, Kaspersky Endpoint Security zablokuje tę akcję i wyświetli powiadomienie (patrz rysunek poniżej).



Powiadomienie Adaptacyjnej kontroli anomalii

Algorytm działania Adaptacyjnej kontroli anomalii

Kaspersky Endpoint Security decyduje, czy zezwolić na lub zablokować działanie skojarzone z regułą opartą o następujący algorytm (patrz rysunek poniżej).



Algorytm działania Adaptacyjnej kontroli anomalii

Ustawienia komponentu Adaptacyjna kontrola anomalii

Parametr	Opis
Raport o stanie reguł	Ten raport zawiera informacje o stanie reguł wykrywania komponentu Adaptacyjna kontrola anomalii (na przykład: <i>Wyłączona</i> lub <i>Zablokuj</i>). Raport jest generowany dla wszystkich grup

<p>Adaptacyjnej kontroli anomalii</p> <p><i>(dostępny tylko w Kaspersky Security Center Console)</i></p>	<p>administracyjnych.</p>
<p>Raport o wywołanych regułach Adaptacyjnej kontroli anomalii</p> <p><i>(dostępny tylko w Kaspersky Security Center Console)</i></p>	<p>Ten raport zawiera informacje o nietypowych działaniach wykrytych przy użyciu komponentu Adaptacyjna kontrola anomalii. Raport jest generowany dla wszystkich grup administracyjnych.</p>
<p>Reguły</p>	<p>Tabela reguł komponentu Adaptacyjna kontrola anomalii. Reguły są tworzone przez specjalistów z Kaspersky w oparciu o typowe scenariusze potencjalnie złośliwej aktywności.</p>
<p>Szablony</p>	<ul style="list-style-type: none"> • Wiadomość dotycząca blokowania. Szablon komunikatu, który jest wyświetlany użytkownikowi po wyzwoleniu reguły komponentu Adaptacyjna kontrola anomalii, która blokuje nietypowe działanie. • Wiadomość do administratora. Szablon wiadomości dla użytkownika, która może zostać wysłana do lokalnego administratora sieci korporacyjnej, jeśli użytkownik uzna, że zablokowanie jest pomyłką. Gdy użytkownik zażąda dostępu, Kaspersky Endpoint Security wyśle zdarzenie do Kaspersky Security Center: Wiadomość do administratora dotycząca zablokowania aktywności aplikacji Opis zdarzenia zawiera wiadomość do administratora z podstawionymi zmiennymi. Możesz przeglądać te zdarzenia w konsoli Kaspersky Security Center przy użyciu wstępnie zdefiniowanego wyboru zdarzeń Żądania użytkowników. Jeśli Twoja organizacja nie ma wdrożyła Kaspersky Security Center lub nie ma połączenia z Serwerem administracyjnym, aplikacja wyśle wiadomość do administratora na podany adres e-mail.

Endpoint Sensor

Endpoint Sensor nie jest zawarty w Kaspersky Endpoint Security 11.4.0.

Możesz zarządzać Endpoint Sensor w konsoli Kaspersky Security Center Web Console i Konsoli administracyjnej Kaspersky Security Center. Nie można zarządzać Endpoint Sensor w konsoli Kaspersky Security Center Cloud Console.

Endpoint Sensor to komponent zaprojektowany do interakcji z Kaspersky Anti Targeted Attack Platform. *Kaspersky Anti Targeted Attack Platform* to rozwiązanie zaprojektowane w celu szybkiego wykrywania złożonych zagrożeń, takich jak ataki ukierunkowane, zaawansowane trwałe zagrożenia (APT), ataki zero-day i inne. Kaspersky Anti Targeted Attack Platform zawiera dwie sekcje funkcjonalne: Kaspersky Anti Targeted Attack (zwany dalej również „KATA”) oraz Kaspersky Endpoint Detection and Response (zwany dalej również „KEDR”). Możesz kupić KEDR osobno. Szczegółowe informacje na temat rozwiązania można znaleźć w [systemie pomocy dla Kaspersky Anti Targeted Attack Platform](#).

Zarządzanie Endpoint Sensor posiada następujące ograniczenia:

- Możesz skonfigurować ustawienia Endpoint Sensor w zasadzie, pod warunkiem że na komputerze jest zainstalowany Kaspersky Endpoint Security w wersji od 11.0.0 do 11.3.0. Aby uzyskać więcej informacji na temat konfigurowania ustawień Endpoint Sensor przy użyciu zasady, zapoznaj się z [artykułami pomocy dotyczącymi poprzednich wersji Kaspersky Endpoint Security](#).
- Jeśli na komputerze jest zainstalowany program Kaspersky Endpoint Security w wersji 11.4.0 i nowszej, nie można skonfigurować ustawień Endpoint Sensor przy użyciu zasady.

Endpoint Sensor jest zainstalowany na komputerach klienckich. Na tych komputerach komponent ciągle monitoruje procesy, aktywne połączenia sieciowe oraz pliki, które są modyfikowane. Endpoint Sensor przekazuje informacje do serwera KATA.

Funkcjonalność komponentu jest dostępna w następujących systemach operacyjnych:

- Windows 7 Service Pack 1 Home / Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2016 Essentials / Standard (64-bit).

Szczegółowe informacje na temat działania KATA można znaleźć w [systemie pomocy dla Kaspersky Anti Targeted Attack Platform](#).

Kaspersky Sandbox

Kaspersky Endpoint Security 11.7.0 teraz zawiera komponent Kaspersky Sandbox. Komponent umożliwia współdziałanie z rozwiązaniem Kaspersky Sandbox. *Rozwiązanie Kaspersky Sandbox* wykrywa i automatycznie blokuje zaawansowane zagrożenia na komputerach. Kaspersky Sandbox analizuje zachowanie obiektów w celu wykrywania szkodliwej aktywności oraz aktywności charakterystycznej dla ataków docelowych ukierunkowanych na infrastrukturę IT organizacji. Kaspersky Sandbox analizuje i skanuje obiekty na specjalnych serwerach z wdrożonymi obrazami wirtualnymi systemów operacyjnych Microsoft Windows (serwery Kaspersky Sandbox). Więcej informacji o rozwiązaniu można znaleźć w *pomocy dla [Kaspersky Sandbox](#)*.

Komponent może być zarządzany tylko przy użyciu konsoli Kaspersky Security Center Web Console. Nie możesz zarządzać tym komponentem przy użyciu Konsoli administracyjnej (MMC).

Ustawienia komponentu Kaspersky Sandbox

Parametr	Opis
Certyfikat TLS serwera	Aby skonfigurować zaufane połączenie z serwerami Kaspersky Sandbox, musisz przygotować certyfikat TLS. Następnie musisz dodać certyfikat do serwerów Kaspersky Sandbox i zasady Kaspersky Endpoint Security. Więcej informacji na temat przygotowywania certyfikatu i dodawania certyfikatu do serwerów znajdziesz w <i>pomocy dla Kaspersky Sandbox</i> .
Limit czasu połączenia dla Kaspersky Sandbox został przekroczony	Limit czasu połączenia dla serwera Kaspersky Sandbox został przekroczony. Po skonfigurowaniu upłynięcia określonej ilości czasu, Kaspersky Endpoint Security wyśle żądanie do następnego serwera. Możesz zwiększyć limit czasu połączenia dla Kaspersky Sandbox, jeśli prędkość Twojego połączenia spada lub jeśli połączenie jest niestabilne. Domyślnie wynosi on 5 sekund.
Kolejka żądań Kaspersky Sandbox	Rozmiar folderu kolejki żądań. Jeśli na komputerze jest dostęp do obiektu (uruchomiony plik wykonywalny lub otwarty dokument, na przykład w formacie DOCX lub PDF), Kaspersky Endpoint Security może także wysłać obiekt do skanowania wykonywanego przez Kaspersky Sandbox. Jeśli istnieje kilka żądań, Kaspersky Endpoint Security tworzy kolejkę żądań. Domyślnie, rozmiar folderu kolejki żądań jest ograniczony do 100 MB. Po osiągnięciu maksymalnego rozmiaru, Kaspersky Sandbox przestanie dodawać nowe żądania do kolejki i wyśle odpowiednie zdarzenie do Kaspersky Security Center. Możesz skonfigurować rozmiar folderu kolejki żądań w zależności od konfiguracji Twojego serwera.
Serwery Kaspersky Sandbox	Ustawienia połączenia z serwerem Kaspersky Sandbox. Serwery używają wdrożonych obrazów wirtualnych systemów operacyjnych Microsoft Windows do uruchamiania obiektów, które muszą zostać przeskanowane. Możesz wprowadzić adres IP (IPv4 lub IPv6) lub w pełni kwalifikowaną nazwę domeny.
Działanie podejmowane w przypadku wykrycia zagrożenia	<p>Przenieś kopię do Kwarantanny, usuń obiekt. Jeśli ta opcja została zaznaczona, Kaspersky Endpoint Security usunie szkodliwy obiekt wykryty na komputerze. Przed usunięciem obiektu Kaspersky Endpoint Security utworzy kopię zapasową w przypadku, gdy obiekt musi zostać przywrócony w późniejszym czasie. Kaspersky Endpoint Security przeniesie kopię zapasową do Kwarantanny.</p> <p>Uruchom skanowanie obszarów krytycznych. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security uruchamia <i>zadanie Skanowanie obszarów krytycznych</i>. Domyślnie, Kaspersky Endpoint Security skanuje pamięć jądra, uruchomione procesy i sektory startowe dysku.</p> <p>Uruchom skanowanie IOC. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security automatycznie tworzy zadanie <i>Skanowanie IOC</i> (<i>autonomiczne zadanie skanowania IOC</i>). Dla tego zadania możesz skonfigurować tryb uruchamiania, obszar skanowania oraz akcję po wykryciu IOC: usunąć obiekt, uruchomić zadanie <i>Skanowanie obszarów krytycznych</i>. Aby zmodyfikować inne ustawienia zadania <i>Skanowanie IOC</i>, przejdź do ustawień zadania.</p>
Obszar skanowania IOC	Krytyczne obszary plików. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security wykonuje skanowanie IOC tylko w krytycznych obszarach plików komputera: pamięci jądra i sektorów startowych.

	Obszary plików na dyskach systemowych urządzenia. Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security nie skanuje IOC na dysku systemowym komputera.
Uruchom skanowanie IOC	<p>Ręcznie. Tryb uruchamiania, w którym możesz ręcznie uruchomić zadanie <i>Skanowanie IOC</i> w wybranym przez siebie momencie.</p> <p>Po wykryciu zagrożenia. Tryb uruchamiania, w którym Kaspersky Endpoint Security automatycznie uruchomi zadanie <i>Skanowanie IOC</i> za każdym razem, gdy zagrożenie zostanie wykryte.</p> <p>Uruchamiaj tylko, jeśli komputer jest w stanie beczynności. Tryb uruchamiania, w którym Kaspersky Endpoint Security uruchomi zadanie <i>Skanowanie IOC</i>, jeśli wygaszacz ekranu jest aktywny lub ekran jest zablokowany. Jeśli użytkownik odblokuje komputer, Kaspersky Endpoint Security wstrzyma zadanie. To oznacza, że wykonanie zadania może zająć kilka dni.</p>

Endpoint Detection and Response

Kaspersky Endpoint Security 11.7.0 posiada teraz wbudowanego agenta dla rozwiązania Kaspersky Endpoint Detection and Response Optimum (zwane dalej „EDR Optimum”). *Kaspersky Endpoint Detection and Response Optimum* to rozwiązanie do ochrony infrastruktury IT organizacji przed zaawansowanymi cyberzagrożeniami. Funkcjonalność rozwiązania łączy automatyczne wykrywanie zagrożeń z możliwością reagowania na te zagrożenia w celu przeciwdziałania zaawansowanym atakom, w tym nowym exploitom, oprogramowaniu ransomware, atakom bezplikowym, a także metodom z użyciem legalnych narzędzi systemowych. Więcej informacji o rozwiązaniu znajdziesz w [pomocy dla Kaspersky Endpoint Detection and Response Optimum](#).

Kaspersky Endpoint Detection and Response Optimum przegląda i analizuje rozwój zagrożeń i zapewnia *personel ds. bezpieczeństwa* lub *Administratora* z informacjami o potencjalnym ataku, które są niezbędne do reagowania w odpowiednim momencie. Kaspersky Endpoint Detection and Response wyświetla szczegóły wykrycia w oddzielnym oknie. *Szczegóły wykrycia* to narzędzie do przeglądania całości zebranych informacji o wykrytym zagrożeniu i zarządzaniu działaniami odpowiedzi. Szczegóły wykrycia obejmują, na przykład, historię plików pojawiających się na komputerze. Więcej informacji o zarządzaniu szczegółami wykrycia można znaleźć w pomocy do [Kaspersky Endpoint Detection and Response Optimum](#).

Komponent może być zarządzany tylko przy użyciu konsoli Kaspersky Security Center Web Console. Nie możesz zarządzać tym komponentem przy użyciu Konsoli administracyjnej (MMC).

Ustawienia Endpoint Detection and Response Optimum

Parametr	Opis
Izolacja sieci	<p>Automatyczna izolacja komputera od sieci w odpowiedzi na wykryte zagrożenia.</p> <p>Jeśli izolacja sieci jest włączona, aplikacja zrywa wszystkie aktywne połączenia i blokuje wszystkie nowe połączenia TCP/IP na komputerze. Aplikacja pozostawia aktywne tylko następujące połączenia:</p> <ul style="list-style-type: none"> • Połączenia znajdujące się w wykluczeniach Izolacji sieci. • Połączenia zainicjowane przez usługi Kaspersky Endpoint Security. • Połączenia zainicjowane przez agenta administracji Kaspersky Security Center.
Automatycznie odblokuj izolowany komputer w ciągu N godzin	Izolacja sieci może zostać wyłączona automatycznie po określonym czasie lub ręcznie. Domyślnie, Kaspersky Endpoint Security wyłączy Izolację sieci 5 godzin od rozpoczęcia izolacji.
Wykluczenia	Lista reguł dla wykluczeń z izolacji sieci. Połączenia sieciowe, które odpowiadają regułom,

<p>Izolacji sieci</p>	<p>nie są blokowane na komputerach, gdy Izolacja sieci jest włączona.</p> <p>Aby skonfigurować wykluczenia izolacji sieci, możesz użyć listy <i>standardowych profili sieciowych</i>. Domyślnie, wykluczenia obejmują profile sieciowe zawierające reguły, które zapewniają nieprzerwane działanie urządzeń z rolami serwera DNS/DHCP i klienta DNS/DHCP. Możesz także ręcznie zmodyfikować ustawienia standardowych profili sieciowych lub zdefiniować wykluczenia.</p> <div style="background-color: #f8d7da; padding: 10px; margin-top: 10px;"> <p>Wykluczenia określone we właściwościach zasady są stosowane tylko wtedy, gdy Izolacja sieci zostaje włączona automatycznie w odpowiedzi na wykryte zagrożenie. Wykluczenia określone we właściwościach komputera są stosowane tylko wtedy, gdy Izolacja sieci zostanie włączona ręcznie we właściwościach komputera w konsoli Kaspersky Security Center.</p> </div>
<p>Zapobieganie wykonywaniu</p>	<p>Kontrola wykonania plików wykonywalnych i skryptów oraz otwarcia plików formatów office. Na przykład, możesz zapobiec wykonaniu aplikacji, które są uznawane za niezabezpieczone na wybranym komputerze. Zapobieganie wykonywaniu obsługuje zestaw rozszerzeń plików pakietu office oraz zestaw interpreterów skryptu.</p>
<p>Akcja podczas wykonywania lub otwierania zabronionego obiektu</p>	<p>Blokuj i zapisz do raportu. W tym trybie aplikacja blokuje wykonanie obiektów lub otwieranie dokumentów, które odpowiadają kryteriom reguły blokowania. Aplikacja publikuje także zdarzenie dotyczące prób wykonania obiektów lub otwarcia dokumentów w Dzienniku zdarzeń Windows oraz dzienniku zdarzeń Kaspersky Security Center.</p> <p>Tylko zapisuj zdarzenia. W tym trybie Kaspersky Endpoint Security publikuje zdarzenie dotyczące prób uruchomienia obiektów wykonywalnych lub otwarcia dokumentów, które odpowiadają kryteriom reguły blokowania, w Dzienniku zdarzeń Windows oraz w Kaspersky Security Center, ale nie blokują próby uruchomienia lub otwarcia obiektu lub dokumentu. Ten tryb jest wybrany domyślnie.</p>
<p>Reguły zapobiegania wykonywaniu</p>	<p>Lista reguł zapobiegania wykonywaniu obiektu. <i>Reguły zapobiegania wykonywaniu</i> to zestaw kryteriów, które są uznawane podczas blokowania. Aplikacja identyfikuje pliki według ich ścieżek lub sum kontrolnych wyliczonych przy użyciu algorytmów haszowania MD5 i SHA256.</p>

Szyfrowanie całego dysku

Możesz wybrać technologię szyfrowania: Kaspersky Disk Encryption lub Szyfrowanie dysków funkcją BitLocker (zwana dalej również "BitLocker").

Kaspersky Disk Encryption

Po zaszyfrowaniu dysków twardech, przy kolejnym uruchomieniu komputera użytkownik musi przejść proces autoryzacji przy użyciu [Agenta autoryzacji](#) przed uzyskaniem dostępu do dysków twardech i załadowaniem systemu operacyjnego. Wymaga to wprowadzenia hasła do tokena lub karty inteligentnej podłączonej do komputera, bądź wpisania nazwy użytkownika i hasła konta Agentu autoryzacji utworzonego przez administratora lokalnej sieci firmowej przy użyciu zadania [Zarządzanie kontem Agentu autoryzacji](#). Konta te są oparte na kontach systemu Microsoft Windows, z poziomu których użytkownik loguje się do systemu operacyjnego. Możesz także [użyć technologii logowania jednokrotnego \(SSO\)](#), która umożliwia automatyczne logowanie do systemu operacyjnego przy użyciu nazwy użytkownika i hasła dla konta Agentu autoryzacji.

Autoryzacja użytkownika w Agencie autoryzacji może przebiegać na dwa sposoby:

- Poprzez wprowadzenie nazwy i hasła konta Agenta autoryzacji, utworzonego przez administratora sieci LAN przy użyciu narzędzi Kaspersky Security Center.
- Poprzez wprowadzenie hasła do tokena lub karty inteligentnej, podłączonych do komputera.

Użycie tokena lub karty inteligentnej jest możliwe tylko wtedy, gdy dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES256. Jeśli dyski twarde komputera zostały zaszyfrowane przy użyciu algorytmu szyfrowania AES56, dodanie pliku certyfikatu elektronicznego do polecenia zostanie odrzucone.

Szyfrowanie dysków funkcją BitLocker

BitLocker to technologia szyfrowania wbudowana w systemy operacyjne Windows. Kaspersky Endpoint Security pozwala kontrolować i zarządzać BitLocker za pomocą Kaspersky Security Center. BitLocker szyfruje woluminy logiczne. Funkcja BitLocker nie może być używana do szyfrowania dysków wymiennych. Więcej informacji na temat BitLocker można znaleźć w [dokumentacji firmy Microsoft](#).

Funkcja BitLocker zapewnia bezpieczne przechowywanie kluczy dostępu za pomocą zaufanego modułu platformy. *Moduł TPM (Trusted Platform Module)* to mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład, do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej. Korzystanie z modułu TPM jest najbezpieczniejszym sposobem przechowywania kluczy dostępu funkcji BitLocker, ponieważ moduł TPM zapewnia weryfikację integralności systemu przed uruchomieniem. Nadal możesz szyfrować dyski na komputerze bez modułu TPM. W takim przypadku klucz dostępu zostanie zaszyfrowany przy użyciu hasła. Funkcja BitLocker używa następujących metod uwierzytelniania:

- TPM.
- TPM i PIN.
- Hasło.

Po zaszyfrowaniu dysku funkcja BitLocker tworzy klucz główny. Kaspersky Endpoint Security wysyła klucz główny do Kaspersky Security Center, abyś mógł [przywrócić dostęp do dysku](#), na przykład, jeśli użytkownik zapomniał hasło.

Jeśli użytkownik zaszyfruje dysk przy użyciu funkcji BitLocker, Kaspersky Endpoint Security wyśle [informacje o szyfrowaniu dysku do Kaspersky Security Center](#). Jednak Kaspersky Endpoint Security nie wyśle klucza głównego do Kaspersky Security Center, więc przywrócenie dostępu do dysku za pomocą Kaspersky Security Center będzie niemożliwe. Aby funkcja BitLocker działała poprawnie z Kaspersky Security Center, [odszyfruj dysk](#) i [ponownie zaszyfruj dysk](#) przy użyciu zasady. Możesz odszyfrować dysk lokalnie lub za pomocą zasady.

Po zaszyfrowaniu systemowego dysku twardego użytkownik musi przejść uwierzytelnianie funkcją BitLocker, aby uruchomić system operacyjny. Po procedurze uwierzytelniania funkcja BitLocker pozwoli użytkownikom zalogować się. Funkcja BitLocker nie obsługuje technologii pojedynczego logowania (SSO).

Jeśli używasz zasad grupy Windows, wyłącz zarządzanie funkcją BitLocker w ustawieniach zasad. Ustawienia zasad Windows mogą kolidować z ustawieniami zasad Kaspersky Endpoint Security. Podczas szyfrowania dysku mogą wystąpić błędy.

Ustawienia komponentu Kaspersky Disk Encryption

Parametr	Opis
----------	------

<p>Tryb szyfrowania</p>	<p>Zaszyfruj wszystkie dyski twarde. Jeśli ten element jest zaznaczony, aplikacja szyfruje wszystkie dyski twarde po zastosowaniu zasady.</p> <div style="background-color: #f8d7da; padding: 10px; margin: 10px 0;"> <p>Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po szyfrowaniu będziesz mógł załadować tylko ten system operacyjny, na którym jest zainstalowana aplikacja.</p> </div> <p>Odszyfruj wszystkie dyski twarde. Jeśli ten element jest zaznaczony, po zastosowaniu zasady aplikacja deszyfruje wszystkie wcześniej zaszyfrowane dyski twarde.</p> <p>Pozostaw niezmienione. Jeśli ten element jest zaznaczony, po zastosowaniu zasady aplikacja pozostawia dyski nienaruszone. Jeśli dysk był zaszyfrowany, pozostanie zaszyfrowany. Jeśli dysk był odszyfrowany, pozostanie odszyfrowany. Ten element jest wybrany domyślnie.</p>
<p>Podczas szyfrowania automatycznie utwórz konta Agenta autoryzacji dla użytkowników systemu Windows</p>	<p>Jeśli to pole jest zaznaczone, aplikacja tworzy konta Agenta autoryzacji w oparciu o listę kont użytkowników systemu Windows na komputerze. Domyślnie, Kaspersky Endpoint Security używa wszystkich kont lokalnych i domenowych, z którymi użytkownik logował się do systemu operacyjnego w ciągu ostatnich 30 dni.</p>
<p>Ustawienia tworzenia konta Agenta autoryzacji</p>	<p>Wszystkie konta na komputerze. Jeśli to pole jest zaznaczone, podczas wykonywania zadania szyfrowania całego dysku program Kaspersky Endpoint Security tworzy konta Agenta autoryzacji dla wszystkich kont komputera, które kiedykolwiek były aktywne.</p> <p>Wszystkie konta domenowe na komputerze. Jeśli to pole jest zaznaczone, podczas wykonywania zadania szyfrowania całego dysku program Kaspersky Endpoint Security tworzy konta Agenta autoryzacji dla wszystkich kont komputera należących do określonej domeny, które kiedykolwiek były aktywne.</p> <p>Wszystkie konta lokalne na komputerze. Jeśli to pole jest zaznaczone, podczas wykonywania zadania szyfrowania całego dysku program Kaspersky Endpoint Security tworzy konta Agenta autoryzacji dla wszystkich kont komputera lokalnego, które kiedykolwiek były aktywne.</p> <p>Lokalny administrator. Jeśli to pole jest zaznaczone, podczas wykonywania zadania szyfrowania całego dysku program Kaspersky Endpoint Security tworzy konto lokalnego administratora.</p> <p>Menedżer komputera. Jeśli to pole jest zaznaczone, podczas wykonywania zadania szyfrowania całego dysku program Kaspersky Endpoint Security tworzy konto Agenta autoryzacji dla konta, którego właściwości w Active Directory pokazują, że jest to konto zarządzające.</p> <p>Aktywne konto. Jeśli to pole jest zaznaczone, podczas wykonywania zadania szyfrowania całego dysku program Kaspersky Endpoint Security automatycznie tworzy konto Agenta autoryzacji dla konta komputera, które jest aktywne podczas wykonywania zadania.</p>
<p>Automatycznie utwórz konta Agenta autoryzacji dla wszystkich użytkowników tego komputera podczas pierwszego logowania</p>	<p>Jeśli to pole jest zaznaczone, aplikacja sprawdza informacje o kontach użytkownika systemu Windows na komputerze przed uruchomieniem Agenta autoryzacji. Jeśli Kaspersky Endpoint Security wykryje konto użytkownika systemu Windows, które nie zawiera konta Agenta autoryzacji, aplikacja utworzy nowe konto do uzyskania dostępu do zaszyfrowanych dysków. Nowe konto Agenta autoryzacji będzie posiadało domyślne ustawienia: tylko logowanie zabezpieczone hasłem oraz zmiana hasła po pierwszej autoryzacji. Dlatego też nie musisz ręcznie dodawać kont Agenta autoryzacji przy użyciu zadania <i>Zarządzanie kontami Agenta autoryzacji</i> dla komputerów z już zaszyfrowanymi dyskami.</p>

<p>Zapisz nazwę użytkownika wprowadzoną w Agencji autoryzacji</p>	<p>Jeśli to pole jest zaznaczone, aplikacja zapisze nazwę konta Agenta autoryzacji. Przy następnej próbie zalogowania się do Agenta autoryzacji z poziomu tego samego konta nie będzie konieczne wpisanie nazwy konta.</p>
<p>Zaszyfruj tylko używaną przestrzeń dyskową</p>	<p>To pole włącza/wyłącza opcję ograniczającą obszar szyfrowania tylko do zajmowanych sektorów dysku twardego. To ograniczenie pozwala na skrócenie czasu szyfrowania.</p> <div data-bbox="395 416 1493 607" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Włączenie lub wyłączenie funkcji Szyfruj tylko zajęta przestrzeń dysku (redukuje czas szyfrowania) po rozpoczęciu szyfrowania nie powoduje zmodyfikowania tego ustawienia, aż do odszyfrowania dysków twardego. Przed rozpoczęciem szyfrowania należy zaznaczyć lub odznaczyć to pole.</p> </div> <p>Jeśli pole jest zaznaczone, zostaną zaszyfrowane tylko te obszary dysku twardego, które są zajęte przez pliki. Kaspersky Endpoint Security automatycznie szyfruje nowe dane po ich dodaniu.</p> <p>Jeśli pole jest odznaczone, cały dysk twardego jest szyfrowany, w tym fragmenty wcześniej usuniętych i zmodyfikowanych plików.</p> <div data-bbox="395 875 1493 1066" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Ta opcja jest zalecana dla nowych dysków twardego, których dane nie zostały zmodyfikowane ani usunięte. Jeśli stosujesz szyfrowanie na dysku twardego, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku twardego. Zapewni to ochronę wszystkich danych, także tych usuniętych, które potencjalnie można odzyskać.</p> </div> <p>Domyślnie pole to nie jest zaznaczone.</p>
<p>Obsługa starszych wersji USB</p>	<p>To pole włącza/wyłącza funkcję Obsługa starszych wersji USB. <i>Obsługa starszych wersji USB to</i> funkcja BIOS/UEFI, która umożliwia korzystanie z urządzeń USB (takich jak token zabezpieczający) w trakcie fazy rozruchu komputera przed uruchomieniem systemu operacyjnego (tryb BIOS). Obsługa starszych wersji USB nie wpływa na obsługę urządzeń USB po uruchomieniu systemu operacyjnego.</p> <p>Jeśli pole jest zaznaczone, obsługa urządzeń USB podczas pierwszego uruchomienia komputera będzie włączona.</p> <div data-bbox="395 1487 1493 1682" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0; background-color: #f8d7da;"> <p>Jeśli funkcja Obsługa starszych wersji USB jest włączona, Agent autoryzacji w trybie BIOS nie obsługuje pracy z tokenami za pośrednictwem USB. Zalecane jest użycie tej opcji tylko wtedy, gdy istnieje problem kompatybilności sprzętowej i tylko dla tych komputerów, na których wystąpił problem.</p> </div>
<p>Ustawienia hasła</p>	<p>Ustawienia siły hasła konta Agenta autoryzacji. Możesz także włączyć korzystanie z technologii jednokrotnego logowania (SSO).</p> <p>Technologia SSO umożliwia użycie tych samych danych uwierzytelniających konta do uzyskania dostępu do dysków twardego i do systemu operacyjnego.</p> <p>Jeśli pole jest zaznaczone, musisz wprowadzić dane uwierzytelniające konta w celu uzyskania dostępu do zaszyfrowanych dysków twardego i automatycznego zalogowania do systemu operacyjnego.</p>

	Jeśli pole jest odznaczone, w celu uzyskania dostępu do zaszyfrowanych dysków twardech i zalogowania do systemu operacyjnego należy oddzielnie wprowadzić dane uwierzytelniające dla uzyskania dostępu do zaszyfrowanych dysków twardech oraz dane uwierzytelniające konta użytkownika systemu operacyjnego.
Treść pomocy	<p>Autoryzacja. Tekst pomocy wyświetlany w oknie Agenta autoryzacji podczas wprowadzania poświadczeń konta.</p> <p>Zmień hasło. Tekst pomocy wyświetlany w oknie Agenta autoryzacji podczas zmiany hasła do konta Agenta autoryzacji.</p> <p>Przywracanie hasła. Tekst pomocy wyświetlany w oknie Agenta autoryzacji podczas odzyskiwania hasła do konta Agenta autoryzacji.</p>

Ustawiania modułu Szyfrowania dysków funkcją BitLocker

Parametr	Opis
Tryb szyfrowania	<p>Zaszyfruj wszystkie dyski twarde. Jeśli ten element jest zaznaczony, aplikacja szyfruje wszystkie dyski twarde po zastosowaniu zasady.</p> <div style="background-color: #f8d7da; padding: 10px; margin: 10px 0;"> <p>Jeśli na komputerze jest zainstalowanych kilka systemów operacyjnych, po szyfrowaniu będziesz mógł załadować tylko ten system operacyjny, na którym jest zainstalowana aplikacja.</p> </div> <p>Odszyfruj wszystkie dyski twarde. Jeśli ten element jest zaznaczony, po zastosowaniu zasady aplikacja deszyfruje wszystkie wcześniej zaszyfrowane dyski twarde.</p> <p>Pozostaw niezmienione. Jeśli ten element jest zaznaczony, po zastosowaniu zasady aplikacja pozostawia dyski nienaruszone. Jeśli dysk był zaszyfrowany, pozostanie zaszyfrowany. Jeśli dysk był odszyfrowany, pozostanie odszyfrowany. Ten element jest wybrany domyślnie.</p>
Włącz korzystanie z uwierzytelniania BitLocker wymagającego wprowadzania danych z klawiatury przed uruchomieniem na tabletach	<p>To pole włącza / wyłącza korzystanie z uwierzytelniania wymagającego wprowadzenia danych przed rozruchem nawet wtedy, gdy platforma nie oferuje takiej możliwości (na przykład klawiatury dotykowe na tabletach).</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Ekran dotykowy komputerów typu tablet nie jest dostępny w środowisku wykonawczym przed uruchomieniem systemu. Aby zakończyć uwierzytelnianie funkcji BitLocker na komputerach typu tablet, użytkownik musi, na przykład, podłączyć klawiaturę USB.</p> </div> <p>Jeśli pole jest zaznaczone, użycie uwierzytelniania wymagającego wprowadzenia danych przed rozruchem jest dozwolone. Zalecane jest korzystanie z tego ustawienia tylko na urządzeniach, na których znajdują się alternatywne narzędzia do wprowadzania danych przed rozruchem, na przykład klawiatura USB będąca dodatkiem do klawiatury dotykowej.</p> <p>Jeśli pole jest odznaczone, szyfrowanie dysków funkcją BitLocker nie jest możliwe na tabletach.</p>
Użyj szyfrowania sprzętowego	Jeśli pole jest zaznaczone, aplikacja stosuje szyfrowanie sprzętu. Umożliwia to przyspieszenie szyfrowania i zużycie mniejszej ilości zasobów.
Szyfruj tylko zajęłą przestrzeń dysku (dla systemu operacyjnego Windows 8 i nowszych)	To pole włącza/wyłącza opcję ograniczającą obszar szyfrowania tylko do zajmowanych sektorów dysku twardego. To ograniczenie pozwala na skrócenie czasu szyfrowania.

Włączenie lub wyłączenie funkcji **Szyfruj tylko zajęta przestrzeń dysku (redukuje czas szyfrowania)** po rozpoczęciu szyfrowania nie powoduje zmodyfikowania tego ustawienia, aż do odszyfrowania dysków twardego. Przed rozpoczęciem szyfrowania należy zaznaczyć lub odznaczyć to pole.

Jeśli pole jest zaznaczone, zostaną zaszyfrowane tylko te obszary dysku twardego, które są zajęte przez pliki. Kaspersky Endpoint Security automatycznie szyfruje nowe dane po ich dodaniu.

Jeśli pole jest odznaczone, cały dysk twardego jest szyfrowany, w tym fragmenty wcześniej usuniętych i zmodyfikowanych plików.

Ta opcja jest zalecana dla nowych dysków twardego, których dane nie zostały zmodyfikowane ani usunięte. Jeśli stosujesz szyfrowanie na dysku twardego, który jest już w użyciu, zalecane jest zaszyfrowanie całego dysku twardego. Zapewni to ochronę wszystkich danych, także tych usuniętych, które potencjalnie można odzyskać.

Domyślnie pole to nie jest zaznaczone.

Ustawienia uwierzytelniania

Użyj hasła (dla systemu operacyjnego Windows 8 i nowszych)

Jeśli ta opcja jest zaznaczona, Kaspersky Endpoint Security wyświetli pytanie o wprowadzenie hasła podczas próby uzyskania dostępu do zaszyfrowanego dysku.

Ta opcja może zostać wybrana, gdy moduł TPM nie jest używany.

Używaj modułu TPM (Trusted Platform Module)

Jeśli ta opcja jest zaznaczona, BitLocker korzysta z modułu TPM (Trusted Platform Module).

Moduł TPM (Trusted Platform Module) to mikroczip zaprojektowany do zapewnienia podstawowych funkcji związanych z bezpieczeństwem (na przykład, do przechowywania kluczy szyfrowania). Trusted Platform Module jest zazwyczaj instalowany w płycie głównej komputera i komunikuje się z wszystkimi pozostałymi komponentami systemu za pośrednictwem magistrali sprzętowej.

Dla komputerów działających pod kontrolą systemu Windows 7 lub Windows Server 2008 R2 dostępne jest tylko szyfrowanie przy użyciu modułu TPM. Jeśli moduł TPM nie jest zainstalowany, szyfrowanie funkcją BitLocker nie jest możliwe. Użycie hasła na tych komputerach nie jest obsługiwane.

Urządzenie posiadające moduł Trusted Platform Module może tworzyć klucze szyfrowania, które mogą zostać odszyfrowane tylko z pomocą urządzenia. TPM szyfruje klucze szyfrowania, korzystając z własnych kluczy głównych magazynowania. Klucz główny magazynowania jest przechowywany w Trusted Platform Module. Zapewnia to dodatkowy poziom ochrony przed próbami zhakowania kluczy szyfrowania.

To ustawienie jest wybrane domyślnie.

Możesz ustawić dodatkową warstwę ochrony dostępu do klucza szyfrowania i zaszyfrować klucz z hasłem lub kodu PIN:

- **Użyj kodu PIN dla TPM.** Jeśli to pole jest zaznaczone, użytkownik może użyć kodu PIN do uzyskania dostępu do klucza szyfrowania przechowywanego w Trusted Platform Module (TPM).

Jeśli to pole jest odznaczone, użytkownicy nie mogą korzystać z kodów PIN. Aby uzyskać dostęp do klucza szyfrowania, użytkownik musi wprowadzić hasło.

Możesz zezwolić użytkownikowi na użycie rozszerzonego kodu PIN.

Rozszerzony kod PIN umożliwia używanie innych znaków jako dodatku do znaków numerycznych: dużych i małych liter alfabetu łacińskiego, znaków specjalnych i spacji.

- **Używaj modułu TPM (Trusted Platform Module); jeśli jest niedostępny - używaj hasła.** Jeśli pole jest zaznaczone, użytkownik może użyć hasła w celu uzyskania dostępu do kluczy szyfrowania, gdy moduł Trusted Platform Module (TPM) jest niedostępny.

Jeśli pole wyboru zostanie odznaczone, a TPM nie jest dostępny, szyfrowanie całego dysku nie rozpocznie się.

Szyfrowanie plików

Możesz [tworzyć listy plików](#) według rozszerzenia lub grup rozszerzeń oraz listy folderów przechowywanych na lokalnych dyskach komputera, a także tworzyć [reguły szyfrowania plików, które są tworzone przez określone aplikacje](#). Po zastosowaniu zasady, Kaspersky Endpoint Security zaszyfruje i odszyfruje następujące pliki:

- Pliki pojedynczo dodane do list elementów przeznaczonych do zaszyfrowania i odszyfrowania;
- Pliki przechowywane w folderach dodanych do list elementów przeznaczonych do zaszyfrowania i odszyfrowania;
- Pliki utworzone przez oddzielne aplikacje.

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Szyfrowanie plików ma następujące funkcje specjalne:

- Kaspersky Endpoint Security szyfruje / deszyfruje pliki w wstępnie określonych folderach tylko dla profili lokalnego użytkownika systemu operacyjnego. Kaspersky Endpoint Security nie szyfruje / deszyfruje plików w predefiniowanych folderach profili użytkownika mobilnego, obowiązkowych profili użytkownika, tymczasowych profili użytkownika lub folderach przekierowanych.
- Kaspersky Endpoint Security nie szyfruje plików, których modyfikacja mogłaby uszkodzić system operacyjny i zainstalowane aplikacje. Na przykład, na liście wykluczeń szyfrowania znajdują się następujące pliki i foldery ze wszystkimi osadzonymi folderami:
 - %WINDIR%;
 - %PROGRAMFILES% i %PROGRAMFILES(X86)%;
 - Pliki rejestru systemu Windows.

Lista wykluczeń z szyfrowania nie może być podglądana ani modyfikowana. Pliki i foldery znajdujące się na liście wykluczeń z szyfrowania mogą być dodawane do listy szyfrowania, ale i tak nie będą szyfrowane podczas wykonywania szyfrowania plików.

Ustawienia komponentu Szyfrowanie plików

Parametr	Opis
Zarządzaj szyfrowaniem	<p>Pozostaw niezmienione. Jeśli ten element jest zaznaczony, Kaspersky Endpoint Security pozostawia pliki i foldery bez zmian, nie szyfrując i nie deszyfrując ich.</p> <p>Szyfrowanie zgodne z regułami. Jeśli wybrano ten element, Kaspersky Endpoint Security szyfruje pliki i foldery zgodnie z regułami szyfrowania, deszyfruje pliki i foldery zgodnie z regułami deszyfrowania, a także reguluje dostęp aplikacji do zaszyfrowanych plików zgodnie z regułami aplikacji.</p> <p>Odszyfruj całe urządzenie. Jeśli ten element jest zaznaczony, Kaspersky Endpoint Security odszyfruje wszystkie zaszyfrowane pliki i foldery.</p>
Reguły szyfrowania	<p>Ta zakładka wyświetla reguły szyfrowania dla plików przechowywanych na dyskach lokalnych. Możesz dodać pliki w następujący sposób:</p> <ul style="list-style-type: none"> <p>Wstępnie określone foldery. Kaspersky Endpoint Security pozwala dodać następujące obszary:</p> <p>Dokumenty. Pliki w standardowym folderze <i>Dokumenty</i> systemu operacyjnego i jego podfolderach.</p> <p>Ulubione. Pliki w standardowym folderze <i>Ulubione</i> systemu operacyjnego i jego podfolderach.</p> <p>Pulpit. Pliki w standardowym folderze <i>Pulpit</i> systemu operacyjnego i jego podfolderach.</p> <p>Pliki tymczasowe. Pliki tymczasowe związane z działaniem aplikacji zainstalowanych na komputerze. Na przykład, aplikacje Microsoft Office tworzą pliki tymczasowe zawierające kopie zapasowe dokumentów.</p> <p>Pliki programu Outlook. Pliki dotyczące działania klienta poczty Outlook: pliki danych (PST), pliki danych offline (OST), pliki książki adresowej offline (OAB) oraz pliki osobistej książki adresowej (PAB).</p> <p>Foldery. Możesz wpisać ścieżkę dostępu do folderu. Dodając ścieżkę folderu, przestrzegaj następujących zasad:</p> <p>Użyj zmiennej środowiskowej (na przykład: %FOLDER%\UserFolder\). Możesz użyć zmiennej środowiskowej tylko raz i tylko na początku ścieżki.</p> <p>Nie używaj ścieżek względnych. Możesz użyć zestawu \. . \ (np. C:\Users\.. \UserFolder\). Zestaw \. . \ oznacza przejście do folderu nadrzędnego.</p> <p>Nie używaj znaków * i ?.</p> <p>Nie używaj ścieżek UNC.</p> <p>Użyj ; lub , jako separatora.</p> <p>Pliki według rozszerzenia. Możesz wybrać grupy rozszerzeń z listy, takie jak <i>Archiwa</i> grup rozszerzeń. Możesz także ręcznie dodać rozszerzenie pliku.</p>
Reguły odszyfrowywania	<p>Ta zakładka wyświetla reguły deszyfrowania dla plików przechowywanych na dyskach lokalnych.</p>
Reguły dla aplikacji	<p>Zakładka wyświetla tabelę zawierającą reguły dostępu do zaszyfrowanych plików dla aplikacji oraz reguły szyfrowania dla plików, które zostały utworzone lub zmodyfikowane przez pojedyncze aplikacje.</p>
Ustawienia hasła pakietu zaszyfrowanego	<p>Wymagania dotyczące siły hasła, jakie mają być spełniane podczas tworzenia zaszyfrowanych pakietów.</p>

Szyfrowanie nośników wymiennych

Ten składnik jest dostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla stacji roboczych. Ten składnik jest niedostępny, jeśli Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows dla serwerów.

Kaspersky Endpoint Security obsługuje szyfrowanie plików w systemach plików FAT32 i NTFS. Jeśli dysk wymienny z nieobsługiwany systemem plików jest podłączony do komputera, zadanie szyfrowania dla tego dysku wymiennego zakończy się błędem, a Kaspersky Endpoint Security przypisze do dysku wymiennego stan tylko do odczytu.

W celu ochrony danych na dyskach wymiennych możesz użyć następujących typów szyfrowania:

- Szyfrowanie całego dysku (FDE).

Szyfrowanie całego dysku wymiennego, w tym systemu plików.

Nie jest możliwy dostęp do zaszyfrowanych danych poza siecią korporacyjną. Dostęp do zaszyfrowanych danych w sieci korporacyjnej jest również niemożliwy, jeśli komputer nie jest podłączony do Kaspersky Security Center (na przykład, na komputerze gościa).

- Szyfrowanie na poziomie plików (FLE).

Szyfrowanie tylko plików na dysku wymiennym. System plików pozostaje niezmienny.

Szyfrowanie plików na dyskach wymiennych umożliwia dostęp do danych poza siecią korporacyjną za pomocą specjalnego trybu zwanego [trybem przenośnym](#).

Podczas szyfrowania Kaspersky Endpoint Security tworzy klucz główny. Kaspersky Endpoint Security zapisuje klucz główny w następujących repozytoriach:

- Kaspersky Security Center.

- Na komputerze użytkownika.

Klucz główny jest szyfrowany za pomocą tajnego klucza użytkownika.

- Na dysku wymiennym.

Klucz główny jest szyfrowany za pomocą klucza publicznego Kaspersky Security Center.

Po zakończeniu szyfrowania dane na dysku wymiennym mogą być dostępne w sieci korporacyjnej tak, jakbyś używał zwykłego niezasyfrowanego dysku wymiennego.

Uzyskiwanie dostępu do zaszyfrowanych danych

Gdy podłączony jest dysk wymienny z zaszyfrowanymi danymi, Kaspersky Endpoint Security wykonuje następujące czynności:

1. Sprawdza klucz główny w lokalnej pamięci na komputerze użytkownika.

Jeśli klucz główny zostanie znaleziony, użytkownik uzyskuje dostęp do danych na dysku wymiennym.

Jeśli klucz główny nie zostanie znaleziony, Kaspersky Endpoint Security wykonuje następujące działania:

a. Wysyła zapytanie do Kaspersky Security Center.

Po otrzymaniu zapytania, Kaspersky Security Center wysyła odpowiedź zawierającą klucz główny.

b. Kaspersky Endpoint Security zapisuje klucz główny w lokalnej pamięci na komputerze użytkownika do późniejszych operacji na zaszyfrowanym dysku wymiennym.

2. Odszyfrowuje dane.

Specjalne funkcje szyfrowania dysku wymiennego

Szyfrowanie dysków wymiennych ma następujące funkcje specjalne:

- Zasada z predefiniowanymi ustawieniami szyfrowania dysku wymiennego zostanie utworzona dla określonej grupy zarządzanych komputerów. Dlatego też, wynik stosowania profilu Kaspersky Security Center, skonfigurowanego dla szyfrowania/deszyfrowania dysków wymiennych zależy od komputera, do którego podłączony jest dysk wymienny.
- Kaspersky Endpoint Security nie szyfruje/deszyfruje plików tylko do odczytu, które są przechowywane na nośnikach wymiennych.
- Następujące typy urządzeń są obsługiwane jako dyski wymienne:
 - Nośniki danych podłączone poprzez magistralę USB
 - Dyski twarde podłączone poprzez magistrale USB i FireWire
 - Dyski SSD podłączone poprzez magistrale USB i FireWire

Ustawienia komponentu Szyfrowanie nośników wymiennych

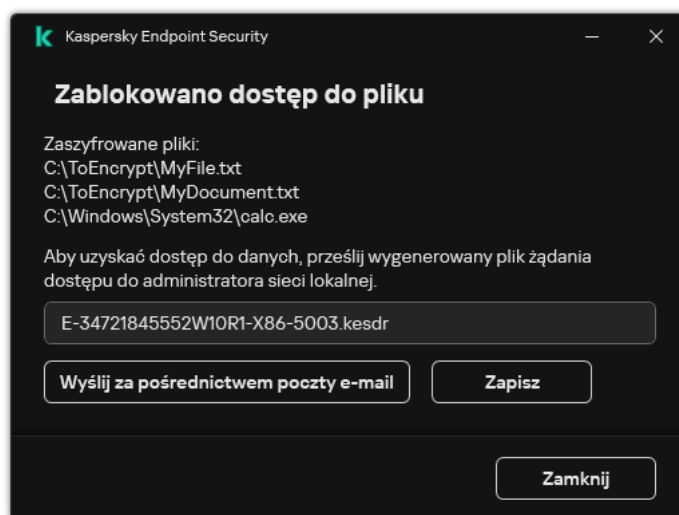
Parametr	Opis
Zarządzaj szyfrowaniem	<p>Zaszyfruj cały dysk wymienny. Jeśli wybrano tę opcję, podczas stosowania zasady z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security szyfruje dyski wymienne sektor po sektorze, w tym ich systemy plików.</p> <p>Zaszyfruj wszystkie pliki. Jeśli wybrano tę opcję, podczas stosowania zasady z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security szyfruje wszystkie pliki przechowywane na dyskach wymiennych. Kaspersky Endpoint Security nie szyfruje ponownie plików, które zostały już zaszyfrowane. Zawartość systemu plików nośników wymiennych, łącznie ze strukturą folderów i z nazwami zaszyfrowanych plików, nie jest szyfrowana i pozostaje dostępna.</p> <p>Zaszyfruj tylko nowe pliki. Jeśli wybrano tę opcję, podczas stosowania zasady z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security szyfruje tylko te pliki, które zostały dodane lub zmodyfikowane na dyskach wymiennych po ostatnim zastosowaniu zasady Kaspersky Security Center. Ten tryb szyfrowania jest wygodny, jeśli dysk wymienny jest wykorzystywany zarówno do celów prywatnych, jak i do celów firmowych. Ten tryb szyfrowania pozwala na zachowanie wszystkich starych plików niezmiennych i zaszyfrowanie tylko tych plików, które użytkownik utworzy w trakcie pracy na komputerze z zainstalowanym Kaspersky Endpoint Security i włączoną funkcją szyfrowania. W rezultacie dostęp do prywatnych plików jest zawsze możliwy, niezależnie od tego, czy Kaspersky Endpoint Security jest zainstalowany na komputerze z włączoną funkcją szyfrowania.</p>

	<p>Odszyfruj cały dysk wymienny. Jeśli wybrano tę opcję, podczas stosowania zasady z określonymi ustawieniami szyfrowania dla dysków wymiennych, Kaspersky Endpoint Security deszyfruje wszystkie zaszyfrowane pliki przechowywane na dyskach wymiennych oraz systemy plików dysków wymiennych, jeśli zostały już wcześniej zaszyfrowane.</p> <p>Pozostaw niezmienione. Jeśli ten element jest zaznaczony, po zastosowaniu zasady aplikacja pozostawia dyski nienaruszone. Jeśli dysk był zaszyfrowany, pozostanie zaszyfrowany. Jeśli dysk był odszyfrowany, pozostanie odszyfrowany. Ten element jest wybrany domyślnie.</p>
<p>Tryb przenośny</p>	<p>Pole to włącza/wyłącza przygotowywanie dysku wymiennego, które pozwala na dostęp do plików przechowywanych na tym dysku wymiennym na komputerach poza siecią korporacyjną.</p> <p>Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security prosi użytkownika o podanie hasła przed zaszyfrowaniem plików na dysku wymiennym po zastosowaniu zasady. Hasło jest niezbędne do uzyskania dostępu do plików zaszyfrowanych na dysku wymiennym na komputerach poza siecią korporacyjną. Możesz skonfigurować siłę hasła.</p> <p>Tryb przenośny jest dostępny dla trybów Szyfruj wszystkie pliki lub Szyfruj tylko nowe pliki.</p>
<p>Zaszyfruj tylko używaną przestrzeń dyskową</p>	<p>To pole włącza / wyłącza tryb szyfrowania, w którym tylko zajmowane sektory dysku zostaną zaszyfrowane. Ten tryb jest zalecany dla nowych dysków, których dane nie zostały zmodyfikowane ani usunięte.</p> <p>Jeśli pole jest zaznaczone, zostaną zaszyfrowane tylko te obszary dysku, które są zajęte przez pliki. Kaspersky Endpoint Security automatycznie szyfruje nowe dane po ich dodaniu.</p> <p>Jeśli pole jest odznaczone, cały dysk jest szyfrowany, w tym fragmenty wcześniej usuniętych i zmodyfikowanych plików.</p> <p>Możliwość szyfrowania tylko zajętego miejsca jest dostępna tylko dla trybu Szyfruj cały dysk wymienny.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Po uruchomieniu szyfrowania, włączenie/wyłączenie funkcji Zaszyfruj tylko używaną przestrzeń dyskową nie zmieni tego ustawienia. Przed rozpoczęciem szyfrowania należy zaznaczyć lub odznaczyć to pole.</p> </div>
<p>Reguły szyfrowania dla wybranych urządzeń</p>	<p>Ta tabela zawiera urządzenia, dla których zdefiniowano niestandardowe reguły szyfrowania. Możesz utworzyć reguły szyfrowania dla poszczególnych dysków wymiennych na następujące sposoby:</p> <ul style="list-style-type: none"> • Dodaj dysk wymienny z listy zaufanych urządzeń dla Kontroli urządzeń. • Ręcznie dodaj dysk wymienny: <ul style="list-style-type: none"> • Według identyfikatora urządzenia (identyfikator sprzętu lub HWID) • Według modelu urządzenia identyfikator producenta (VID) oraz identyfikator produktu (PID)
<p>Zezwól na szyfrowanie dysków wymiennych</p>	<p>Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security szyfruje dyski wymienne, nawet jeśli nie ma połączenia z Kaspersky Security Center. W tym przypadku dane wymagane do odszyfrowania nośnika wymiennego są przechowywane na dysku twardym komputera, do którego podłączony jest nośnik wymienny, i nie są przesyłane do Kaspersky Security Center.</p>

w trybie offline	Jeśli pole to nie jest zaznaczone, Kaspersky Endpoint Security nie szyfruje dysków wymiennych bez połączenia z Kaspersky Security Center.
Ustawienia hasła trybu przenośnego	Ustawienia siły hasła dla Przenośnego menedżera plików.

Szablony (szyfrowanie danych)

Po zaszyfrowaniu danych Kaspersky Endpoint Security może ograniczyć dostęp do danych, na przykład, ze względu na zmianę infrastruktury organizacji i zmianę na Serwerze administracyjnym Kaspersky Security Center. Jeśli użytkownik nie ma dostępu do zaszyfrowanych danych, może poprosić administratora o dostęp do danych. Innymi słowy, użytkownik musi wysłać plik żądania dostępu do administratora. Użytkownik musi następnie przesłać plik odpowiedzi otrzymany od administratora do Kaspersky Endpoint Security. Kaspersky Endpoint Security pozwala poprosić administratora o dostęp do danych za pośrednictwem poczty elektronicznej (patrz rysunek poniżej).



Prośenie o dostęp do zaszyfrowanych danych

Udostępniono szablon do zgłaszania braku dostępu do zaszyfrowanych danych. Dla wygody użytkownika możesz wypełnić następujące pola:

- **Do.** Wprowadź adres e-mail grupy administratorów z uprawnieniami do funkcji szyfrowania danych.
- **Użytkownik.** Wprowadź temat wiadomości e-mail z prośbą o dostęp do zaszyfrowanych plików. Możesz, na przykład, dodawać znaczniki, aby filtrować wiadomości.
- **Wiadomość.** W razie potrzeby zmień treść wiadomości. Możesz użyć zmiennych, aby uzyskać niezbędne dane (na przykład: zmienna % USER_NAME%).

Wykluczenia

Strefa zaufana jest utworzoną przez administratora listą obiektów i aplikacji, które nie są monitorowane przez Kaspersky Endpoint Security.

Administrator tworzy strefę zaufaną, biorąc pod uwagę cechy i funkcje używanych obiektów oraz zainstalowanych aplikacji. Umieszczenie obiektów i aplikacji w strefie zaufanej może być konieczne, gdy Kaspersky Endpoint Security blokuje dostęp do określonego obiektu lub aplikacji, które według Ciebie są nieszkodliwe. Administrator może także zezwolić użytkownikowi na utworzenie własnej lokalnej strefy zaufanej dla określonego komputera. W ten sposób użytkownicy mogą utworzyć swoje własne lokalne listy wykluczeń i zaufanych aplikacji jako dodatek do ogólnej strefy zaufanej w zasadzie.

Wykluczenia ze skanowania

Wykluczenie ze skanowania to zestaw warunków, które muszą być spełnione, aby Kaspersky Endpoint Security nie skanował określonego obiektu w poszukiwaniu wirusów i innych zagrożeń.

Wykluczenia ze skanowania zapewniają możliwość bezpiecznej pracy z legalnymi aplikacjami, które mogą zostać wykorzystane przez hakerów do uszkodzenia komputera lub danych. Nie posiadają one żadnych szkodliwych funkcji, ale mogą zostać wykorzystane przez cyberprzestępców. Szczegółowe informacje o legalnym oprogramowaniu, które może zostać użyte przez cyberprzestępców do uszkodzenia komputera lub danych osobistych użytkownika, znajdują się na [stronie internetowej Encyklopedii IT Kaspersky](#).

Takie aplikacje mogą być blokowane przez program Kaspersky Endpoint Security. Aby zapobiec blokowaniu tych aplikacji, możesz skonfigurować wykluczenia ze skanowania dla używanych aplikacji. W tym celu dodaj do strefy zaufanej nazwę lub maskę nazwy zgodną z klasyfikacją Encyklopedii IT Kaspersky. Na przykład, często używasz aplikacji Radmin do zdalnego zarządzania komputerami. Kaspersky Endpoint Security wykrywa ten rodzaj aktywności aplikacji jako podejrzany i może go zablokować. Aby zapobiec blokowaniu aplikacji, utwórz wykluczenie ze skanowania z nazwą lub maską nazwy z Encyklopedii IT Kaspersky.

Jeśli na komputerze jest zainstalowana aplikacja, która gromadzi informacje i wysyła je do przetworzenia, Kaspersky Endpoint Security może zaklasyfikować tę aplikację jako szkodliwe oprogramowanie. Aby tego uniknąć, możesz wykluczyć tę aplikację ze skanowania, konfigurując Kaspersky Endpoint Security w sposób opisany w dokumencie.

Wykluczenia ze skanowania mogą być używane przez następujące komponenty i zadania aplikacji, które zostały skonfigurowane przez administratora systemu:

- [Wykrywanie zachowań](#).
- [Ochrona przed exploitami](#).
- [Ochrona przed włamaniami](#).
- [Ochrona plików](#).
- [Ochrona WWW](#).
- [Ochrona poczty](#).
- [Zadania skanowania](#).

Lista zaufanych aplikacji

Lista zaufanych aplikacji jest listą aplikacji, których aktywność sieciowa i plikowa (włączając w to szkodliwą aktywność) oraz dostęp do rejestru systemowego nie są monitorowane przez Kaspersky Endpoint Security. Domyślnie program Kaspersky Endpoint Security skanuje obiekty otwierane, uruchamiane lub zapisywane przez proces dowolnej aplikacji i monitoruje aktywność wszystkich aplikacji oraz ruch sieciowy będący wynikiem ich działania. Jednakże aplikacja, która została dodana do listy zaufanych aplikacji zostanie wykluczona ze skanowań wykonywanych przez Kaspersky Endpoint Security.


Jeżeli uważasz, że obiekty używane przez Notatnik firmy Microsoft Windows są nieszkodliwe i nie wymagają skanowania, dodaj Notatnik firmy Microsoft Windows do listy zaufanych aplikacji. Podczas skanowania pomijane będą obiekty używane przez ten program.

Oprócz tego pewne akcje zaklasyfikowane przez Kaspersky Endpoint Security jako podejrzane mogą być traktowane przez inne aplikacje jako nieszkodliwe. Na przykład przechwytywanie danych wprowadzanych z klawiatury jest charakterystyczne dla aplikacji, które automatycznie przełączają układ klawiatury (np. Punto Switcher). Aby korzystać z właściwości takich aplikacji i wyłączyć monitorowanie ich aktywności, dodaj je do listy zaufanych aplikacji.

Wykluczenie zaufanych aplikacji ze skanowania pozwala uniknąć problemów kompatybilności Kaspersky Endpoint Security z innymi programami (np. problem podwójnego skanowania ruchu sieciowego przez Kaspersky Endpoint Security i przez inną aplikację antywirusową), jak również zwiększyć wydajność komputera, która w niektórych sytuacjach osiąga wartość krytyczną.

Należy pamiętać, że pliki wykonywalne oraz procesy zaufanych aplikacji będą nadal skanowane w poszukiwaniu wirusów i szkodliwych programów. Aplikacja może zostać całkowicie wykluczona ze skanowania wykonywanego przez program Kaspersky Endpoint Security przy użyciu wykluczeń ze skanowania.

Ustawienia wykluczeń

Parametr	Opis
Typy wykrywanych obiektów	<p>Bez względu na skonfigurowane ustawienia aplikacji, Kaspersky Endpoint Security zawsze wykrywa i blokuje wirusy, robaki i trojany. Mogą one wyrządzić znaczne szkody w komputerze.</p> <ul style="list-style-type: none">• Wirusy i robaki 

Podkategoria: wirusy i robaki (wirusy_i_robaki)

Poziom zagrożenia: wysoki

Klasyczne wirusy i robaki wykonują akcje nieautoryzowane przez użytkownika. Mogą one tworzyć swoje kopie, które także są zdolne do powielania się.

Klasyczny wirus

Po przeniknięciu klasycznego wirusa do komputera, infekuje on plik, aktywuje się w nim, wykonuje szkodliwe działania i dodaje swoje kopie do innych plików.

Klasyczny wirus rozprzestrzenia się jedynie na zasobach lokalnych komputera; nie może sam przedostać się na inne komputery. Przedostanie się takiego wirusa na inny komputer jest możliwe, jeśli doda on swoją kopię do pliku przechowywanego w folderze współdzielonym lub na nośniku CD, albo gdy użytkownik wyśle wiadomość z zainfekowanym załącznikiem.

Kod klasycznego wirusa może przedostać się do różnych obszarów komputerów, systemów operacyjnych lub aplikacji. W zależności od środowiska wirusy dzieli się na *wirusy plikowe*, *wirusy sektora startowego*, *wirusy skryptowe* oraz *makrowirusy*.

Wirusy mogą infekować pliki, korzystając z szerokiej gamy technik. *Wirusy nadpisujące* zapisują swój kod na kodzie zainfekowanego pliku, wymazując jego zawartość. Zainfekowany plik przestaje poprawnie działać oraz nie ma możliwości jego przywrócenia. *Wirusy pasożyty* modyfikują pliki, zezwalając na ich pełne lub częściowe działanie. *Wirusy towarzysze* nie modyfikują plików, lecz tworzą ich kopie. Kiedy otwarty zostanie zainfekowany plik, uruchomiona zostanie jego kopia (czyli wirus). Można wyróżnić również następujące typy wirusów: *wirusy-odsyłacze*, *wirusy plików OBJ*, *wirusy bibliotek LIB*, *wirusy infekujące kody źródłowe* oraz wiele innych.

Robak

Podobnie jak w przypadku klasycznego wirusa, kod robaka zostaje aktywowany i wykonuje on szkodliwe działania po przeniknięciu do komputera. Robaki noszą taką nazwę z powodu swojej zdolności do "przepędzania" z jednego komputera na inny i rozprzestrzeniania swoich kopii za pośrednictwem wielu kanałów danych bez wiedzy użytkownika.

Główną cechą, która umożliwia rozróżnianie typów robaków, jest ich sposób rozprzestrzeniania się. Następująca tabela zawiera przegląd różnych typów robaków, klasyfikowanych zgodnie ze sposobem rozprzestrzeniania się.

Sposoby rozprzestrzeniania się robaka

Typ	Nazwa	Opis
Email-Worm	Email-Worm	Rozprzestrzeniają się poprzez pocztę elektroniczną.

		<p>Zainfekowana wiadomość zawiera załączony plik z kopią robaka lub odnośnik do pliku znajdującego się na stronie internetowej, która może być albo przechwycona przez hakerów, albo stworzona specjalnie w tym celu. Jeśli otworzysz zainfekowany plik, robak zostanie aktywowany. Po kliknięciu odsyłacza, pobraniu i otwarciu pliku, robak również rozpoczyna swoją szkodliwą działalność. Następnie zaczyna rozprzestrzeniać swoje kopie, wyszukując kolejne adresy e-mail i wysyłając na nie zainfekowane wiadomości.</p>
IM-Worm	Robaki klientów komunikatorów internetowych	<p>Rozprzestrzeniają się poprzez klienty komunikatorów internetowych.</p> <p>Z reguły robaki te za pośrednictwem listy kontaktów użytkownika wysyłają wiadomości zawierające odnośnik do pliku ze swoją kopią. Po pobraniu i otwarciu takiego pliku przez użytkownika, robak jest aktywowany.</p>
IRC-Worm	Robaki czatu internetowego	<p>Rozprzestrzeniają się za pośrednictwem kanału IRC (Internet Relay Chats) – czyli usługi sieciowej pozwalającej na komunikowanie się w internecie w czasie rzeczywistym.</p> <p>Robaki te publikują w czacie internetowym pliki zawierające ich kopie lub odnośniki do pliku. Po pobraniu i otwarciu takiego pliku przez użytkownika, robak jest aktywowany.</p>
Net-Worm	Robaki sieciowe	<p>Rozprzestrzeniają się one w sieciach komputerowych.</p> <p>W przeciwieństwie do innych rodzajów robaków, typowy robak sieciowy rozprzestrzenia się bez udziału użytkownika. Skanuje on sieć lokalną w poszukiwaniu komputerów z programami zawierającymi luki. W tym celu wysyła on specjalny pakiet sieciowy (exploit) zawierający kod robaka lub część kodu. Jeśli komputer posiadający luki znajduje się w sieci, otrzyma taki pakiet sieciowy. Po przeprowadzeniu pełnej penetracji komputera, jest on aktywowany.</p>
P2P-Worm	Robaki sieci wymiany plików	<p>Rozprzestrzeniają się one w sieciach peer-to-peer.</p> <p>Aby dostać się do sieci P2P, robak kopiuje się do foldera wymiany plików, który zazwyczaj znajduje się na komputerze użytkownika. Sieć P2P wyświetli informacje o tym pliku, aby użytkownik "znalazł" zainfekowany plik w sieci, pobrał go i otworzył.</p> <p>Bardziej zaawansowane robaki emulują protokół sieciowy konkretnej sieci P2P: wyświetlają pozytywne wyniki wyszukiwanego obiektu i proponują pobranie swoich własnych kopii.</p>
Robak	Inne rodzaje robaków	<p>Inne rodzaje robaków obejmują:</p> <ul style="list-style-type: none"> • Robaki rozprzestrzeniające swoje kopie w zasobach sieciowych. Przy użyciu funkcji systemu operacyjnego skanują dostępne

foldery sieciowe, łączą się z komputerami w Internecie i próbują uzyskać pełen dostęp do ich dysków. W przeciwieństwie do opisanych wyżej robaków, inne typy robaków nie aktywują się automatycznie, lecz w momencie, gdy użytkownik otworzy plik zawierający kopię robaka.

- Robaki, które nie rozprzestrzeniają się w żaden z powyższych sposobów (na przykład te robaki, które rozprzestrzeniają się poprzez telefony komórkowe).

- [Trojany \(w tym oprogramowanie typu ransomware\)](#) 

Podkategoria: Trojany

Poziom zagrożenia: wysoki

W przeciwieństwie do wirusów i robaków, trojany nie tworzą swoich kopii. Przenikają one do komputera, na przykład, za pośrednictwem wiadomości e-mail lub przeglądarki internetowej po otwarciu zainfekowanej strony. Trojany uruchamiają się przy udziale użytkownika. Zaczynają wykonywać szkodliwe działania zaraz po uruchomieniu.

Różne programy typu trojan zachowują się odmiennie na zainfekowanych komputerach. Głównym zadaniem trojanów jest blokowanie, modyfikowanie lub niszczenie informacji, wyłączanie komputera lub sieci. Poza tym, trojany otrzymują lub wysyłają pliki, uruchamiają je, wyświetlają wiadomości na ekranie, pobierają i instalują aplikacje, uruchamiają ponownie komputer oraz żądają połączenia ze stroną internetową.

Hakerzy często używają "zestawów" trojanów.

Typowe zachowanie trojanów opisane jest w poniższej tabeli.

Typy zachowań trojanów na zainfekowanym komputerze

Typ	Nazwa	Opis
Trojan-ArcBomb	Trojany – "archiwa-bomby"	Archiwa, które po rozpakowaniu zwiększają swój rozmiar, co zakłóca działanie komputera. Podczas próby rozpakowania takiego archiwum komputer może spowolnić swoje działanie lub całkowicie się zawiesić, a dysk twardy może zostać wypełniony "pustymi" danymi. Archiwa-bomby są szczególnie niebezpieczne dla serwerów poczty i plików. Jeśli serwer korzysta z automatycznego systemu przetwarzania informacji przychodzących, archiwum-bomba może zatrzymać jego działanie.
Backdoor	Trojany do zdalnej administracji	Uważa się, że jest to najbardziej niebezpieczny rodzaj trojanów. Dzięki swoim funkcjom są one podobne do programów służących do zdalnej administracji aplikacji zainstalowanych na komputerach. Trojany instalują się na komputerze bez wiedzy użytkownika i pozwalają hakerowi na jego zdalne zarządzanie.
Trojan	Trojany	Do trojanów zaliczają się następujące szkodliwe aplikacje: <ul style="list-style-type: none">• Klasyczne trojany. Wykonują tylko podstawowe funkcje charakterystyczne dla trojanów: blokują, modyfikują lub niszczą informacje, wyłączają komputery lub sieci. W odróżnieniu od trojanów

		<p>opisanych w tabeli, nie charakteryzują się żadnymi zaawansowanymi funkcjami.</p> <ul style="list-style-type: none"> • Wszechstronne trojany. Posiadają zaawansowane funkcje typowe dla kilku rodzajów trojanów.
Trojan-Ransom	Trojany przeznaczone do wyłudzenia pieniędzy	Jako "zakładników" biorą one informacje użytkownika, modyfikują lub blokują je, albo tak wpływają na działanie komputera, że użytkownik nie może korzystać z informacji. Cyberprzestępca żąda okupu od użytkownika, obiecując, że wyśle aplikację, która przywróci działanie komputera oraz przechowywane na nim dane.
Trojan-Clicker	Trojany klikające	<p>Łączą się one ze stronami internetowymi albo przez wysłanie polecenia do przeglądarki albo przez zmianę adresów stron znajdujących się w plikach systemowych.</p> <p>Przy użyciu tych programów hakerzy przeprowadzają ataki sieciowe i zwiększają ranking stron internetowych celem zwiększenia liczby wyświetlania banerów reklamowych.</p>
Trojan-Downloader	Trojany pobierające	Uzyskują dostęp do strony internetowej cyberprzestępcy, pobierają z niej szkodliwe aplikacje i instalują je na komputerze użytkownika. Mogą zawierać nazwę pliku szkodliwej aplikacji do pobrania lub uzyskać ją z otwartej strony internetowej.
Trojan-Dropper	Trojany droppery	<p>Zawierają inne trojany, które instalują na dysku twardym.</p> <p>Hakerzy mogą użyć tego typu trojanów do następujących celów:</p> <ul style="list-style-type: none"> • Zainstalowania szkodliwej aplikacji bez wiedzy użytkownika: Trojan-Dropper to typ programów, które nie wyświetlają żadnych wiadomości lub wyświetlają fałszywe komunikaty informujące, na przykład, o błędzie w archiwum lub niekompatybilnej wersji systemu operacyjnego. • Ochrony innych znanych szkodliwych aplikacji przed wykryciem przez ochronę komputera: nie wszystkie programy antywirusowe są w stanie wykryć szkodliwą aplikację wewnątrz aplikacji Trojan-Dropper.
Trojan-Notifier	Trojany powiadamiające	Informują hakera o możliwości dostępu do zainfekowanego komputera, wysyłając do

		<p>niego informacje o tym komputerze: adres IP, numer otwartego portu lub adres e-mail. Komunikują się z hakerem, na przykład, za pośrednictwem wiadomości e-mail, serwera FTP lub jego strony internetowej.</p> <p>Trojany typu Notifier często są wykorzystywane w zestawach złożonych z kilku trojanów. Powiadamiają one hakera, że inne trojany zostały pomyślnie zainstalowane na komputerze użytkownika.</p>
Trojan-Proxy	Trojany proxy	Umożliwiają one hakerowi uzyskanie anonimowego dostępu do stron internetowych przy użyciu komputera użytkownika i są często używane do wysyłania spamu.
Trojan-PSW	Oprogramowanie kradnące hasła	<p>Oprogramowanie kradnące hasła to rodzaj trojanów kradnących konta użytkownika, na przykład dane rejestracyjne oprogramowania. Takie trojany odnajdują w plikach systemowych i rejestrze poufne dane, a następnie wysyłają je do atakującego, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.</p> <p>Niektóre z tych trojanów podzielone są na kategorie oddzielnych typów opisanych w tej tabeli. Należą do nich Trojany kradnące konta bankowe (Trojan-Banker), trojany kradnące informacje od użytkowników komunikatorów internetowych (Trojan-IM) oraz trojany kradnące informacje od graczy online (Trojan-GameThief).</p>
Trojan-Spy	Trojany szpiegujące	Szpiegują one użytkownika, zbierając informacje o jego działaniach podczas pracy na komputerze. Mogą przechwytywać dane wprowadzane przez użytkownika przy użyciu klawiatury, tworzyć zrzuty ekranu lub tworzyć listę aktywnych aplikacji. Po zebraniu informacji, wysyłają je do hakera, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Trojan-DDoS	Ataki sieciowe	Wysyłają one liczne żądania z komputera użytkownika na serwer zdalny. Serwer nie ma wystarczającej ilości zasobów do przetworzenia wszystkich żądań, w rezultacie przestaje działać (Denial-of-Service lub DoS). Hakerzy często infekują wiele komputerów dzięki takim programom, przez co mogą wykorzystać te komputery do jednoczesnego ataku na pojedynczy serwer.

		Programy DoS przeprowadzają atak z jednego komputera za wiedzą użytkownika. Programy DDoS (Distributed DoS) przeprowadzają rozproszone ataki z różnych komputerów bez wiedzy użytkownika zainfekowanego komputera.
Trojan-IM	Trojany kradnące informacje od użytkowników komunikatorów internetowych	Kradną numery kont i hasła użytkowników klientów komunikatorów internetowych. Przesyłają dane hakerowi, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Rootkit	Rootkity	Ukrywają inne szkodliwe aplikacje i ich aktywność, przedłużając ich obecność w systemie. Mogą również ukrywać pliki i procesy w pamięci zainfekowanego komputera lub kluczach rejestru. Rootkity mogą ukrywać wymianę danych pomiędzy aplikacjami znajdującymi się na komputerze użytkownika i innymi komputerami podłączonymi do sieci.
Trojan-SMS	Trojany wysyłające wiadomości SMS	Infekują one telefony komórkowe, wysyłając wiadomości SMS na numery o podwyższonej opłacie.
Trojan-GameThief	Trojany kradnące informacje od osób grających w sieci	Kradną dane uwierzytniające kont osób grających w sieci, po czym wysyłają je hakerowi za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej.
Trojan-Banker	Trojany kradnące konta bankowe	Kradną dane konta bankowego lub dane systemu płatności elektronicznych, po czym wysyłają je cyberprzestępcy za pośrednictwem poczty elektronicznej, serwera FTP, jego strony internetowej lub przy użyciu innych metod.
Trojan-Mailfinder	Trojany zbierające adresy e-mail	Zbierają one adresy e-mail przechowywane na komputerze i wysyłają je hakerowi, na przykład, za pośrednictwem poczty elektronicznej, serwera FTP lub jego strony internetowej. Na zebrane adresy hakerzy mogą wysłać spam.

- [Szkodliwe narzędzia](#) 

Podkategoria: Szkodliwe narzędzia

Poziom zagrożenia: średni

W odróżnieniu od innych typów szkodliwego oprogramowania, szkodliwe narzędzia nie wykonują swoich akcji zaraz po uruchomieniu. Mogą być bezpiecznie przechowywane i uruchamiane na komputerze użytkownika. Hakerzy często używają funkcji tych programów do tworzenia wirusów, robaków i trojanów oraz do przeprowadzania ataków sieciowych na serwery zdalne, łamania zabezpieczeń komputerów lub wykonywania innych szkodliwych działań.

Różne funkcje szkodliwych narzędzi pogrupowane są według typów opisanych w poniższej tabeli.

Funkcje szkodliwych narzędzi

Typ	Nazwa	Opis
Konstruktor	Konstruktory	Umożliwiają utworzenie nowych wirusów, robaków i trojanów. Niektóre konstruktory posiadają standardowy interfejs oparty na oknach, w którym użytkownik może wybrać typ szkodliwej aplikacji, jaki chce stworzyć, sposób przeciwdziałania debuggerom oraz inne funkcje.
Dos	Ataki sieciowe	Wysyłają one liczne żądania z komputera użytkownika na serwer zdalny. Serwer nie ma wystarczającej ilości zasobów do przetworzenia wszystkich żądań, w rezultacie przestaje działać (Denial-of-Service lub DoS).
Exploit	Exploity	Exploit jest zestawem danych lub kodem programu używającym luki aplikacji, w której jest przetwarzany, do wykonania szkodliwych działań na komputerze. Na przykład, exploit może odczytywać lub zapisywać pliki lub uzyskiwać dostęp do "zainfekowanych" stron internetowych. Różne exploity używają luk w różnych aplikacjach lub usługach sieciowych. Wyglądający jak pakiet sieciowy exploit wysyłany jest przez sieć w poszukiwaniu takich komputerów, których usługi sieciowe posiadają luki. Exploit w pliku DOC używa luk występujących w edytorach tekstu. Po otwarciu przez użytkownika zainfekowanego pliku, może on zacząć wykonywać zaprogramowane przez hakera działania. Exploit osadzony w wiadomości elektronicznej wyszukuje luki w dowolnym kliencie pocztowym. Po otwarciu przez użytkownika zainfekowanego pliku w tym programie pocztowym, wykonuje on szkodliwe działanie.

		Robaki Net-Worms rozprzestrzeniają się w sieci przy pomocy exploitów. <i>Exploity</i> Nuker są pakietami sieciowymi wyłączającymi komputery.
FileCryptor	Narzędzia szyfrujące	Szyfrują one inne szkodliwe aplikacje, aby ukryć je przed programem antywirusowym.
Flooder	Programy "zaśmiecające" sieci	<p>Wysyłają one wiele wiadomości przez kanały sieciowe. Do tego typu narzędzi należy, na przykład, program zaśmiecający Internet Relay Chats (IRC).</p> <p>Wśród narzędzi typu Flooder nie ma programów "zaśmiecających" kanały używane przez programy pocztowe, komunikatory internetowe i systemy komunikacji mobilnej. Programy te wyróżnione są jako oddzielne typy opisane w tej tabeli (Email-Flooder, IM-Flooder oraz SMS-Flooder).</p>
HackTool	Narzędzia hakerskie	Pozwalają na złamanie zabezpieczeń komputera, na którym są zainstalowane, lub na zaatakowanie innego komputera (na przykład, dodając nowe konta systemowe bez wiedzy użytkownika lub wymazując logi systemowe, aby ukryć ślady obecności w systemie operacyjnym). Ten typ narzędzi zawiera sniffery posiadające szkodliwe funkcje, jak choćby przechwytywanie haseł. Sniffery to programy umożliwiające przeglądanie ruchu sieciowego.
Hoax	Żarty (Hoaxes)	Alarmują użytkownika przy użyciu wiadomości podobnej do tej, która używana jest w przypadku wykrycia wirusa: mogą "wykryć wirusa" w nienaruszonym pliku lub powiadomić o formatowaniu dysku, które w rzeczywistości nie ma miejsca.
Spoofier	Narzędzia służące do spoofingu	Wysyłają wiadomości i żądania sieciowe z fałszywym adresem nadawcy. Hakerzy używają narzędzi do spoofingu, na przykład, aby móc podać się za prawdziwych nadawców wiadomości.
VirTool	Narzędzia do modyfikowania szkodliwych aplikacji	Umożliwiają modyfikowanie innego szkodliwego oprogramowania w celu ukrycia go przed aplikacjami antywirusowymi.
Email-Flooder	Programy "zaśmiecające" adresy e-mail	"Zaśmiecają" różne adresy e-mail poprzez wysyłanie na nie licznych wiadomości. Duża liczba wiadomości przychodzących uniemożliwia przejrzanie użytecznych wiadomości znajdujących się w skrzynce odbiorczej.
IM-Flooder	Programy "zaśmiecające" ruch wiadomościami	Wysyłają niechciane wiadomości do użytkowników klientów komunikatorów. Duża liczba odbieranych wiadomości

	klientów komunikatorów internetowych	uniemożliwia przeczytanie użytecznych wiadomości.
SMS-Flooder	Programy "zaśmiecające" ruch wiadomościami SMS	Wysyłają one liczne wiadomości SMS na telefony komórkowe.

- [Adware](#)

Podkategoria: oprogramowanie reklamujące (Adware);

Poziom zagrożenia: średni

Oprogramowanie Adware wyświetla informacje reklamowe użytkownikowi. Programy adware wyświetlają banery reklamowe w interfejsach innych programów i przekierowują wyszukiwanie na strony reklamowe. Niektóre z nich zbierają informacje marketingowe o użytkowniku i wysyłają je do programisty. Do gromadzonych informacji mogą należeć: nazwy stron odwiedzanych przez użytkownika lub wyszukiwana przez niego treść. W odróżnieniu od programów typu Trojan-Spy, programy adware przesyłają te informacje do twórcy za zgodą użytkownika.

- [Auto-dialery](#)

Podkategoria: legalne oprogramowanie, które może zostać wykorzystane przez cyberprzestępców do uszkodzenia komputera i prywatnych danych.

Poziom zagrożenia: średni

Wiele z tych programów to nieszkodliwe oprogramowanie, z którego korzysta wielu użytkowników. Do tych programów zaliczają się: klienty IRC, auto-dialery, programy pobierające pliki, monitory aktywności systemu komputerowego, narzędzia do haseł, serwery usług FTP, HTTP i Telnet.

Jednakże, jeśli haker uzyska dostęp do tego typu programów lub jeśli zainstaluje te programy na komputerze użytkownika, to niektóre z ich funkcji mogą zostać użyte do naruszenia ochrony.

Aplikacje te mają różne funkcje; ich typy zostały opisane w poniższej tabeli.

Typ	Nazwa	Opis
Client-IRC	Klienty czatów internetowych	Użytkownicy instalują programy tego typu, aby móc rozmawiać z innymi w czasie rzeczywistym. Hakerzy używają ich do rozsyłania szkodliwych programów.
Dialer	Auto-dialery	Mogą nawiązywać połączenie telefoniczne za pośrednictwem modemu w trybie ukrycia.
Downloader	Programy do pobierania	Mogą pobierać pliki ze stron internetowych w trybie ukrycia.
Monitor	Programy do monitorowania	Umożliwiają monitorowanie aktywności na komputerze, na którym są zainstalowane (sprawdzają, które aplikacje są aktywne i w jaki sposób wymieniają dane z aplikacjami zainstalowanymi na innych komputerach).
PSWTool	Programy do przywracania haseł	Umożliwiają przeglądanie i przywracanie zapomnianych haseł. Hakerzy umieszczają je na komputerze w tym samym celu, w sposób niezauważalny dla użytkownika.
RemoteAdmin	Programy do zdalnej administracji	Są używane przez administratorów systemów. Programy te pozwalają uzyskać dostęp do interfejsu zdalnego komputera w celu jego monitorowania i zarządzania. W tym właśnie celu hakerzy niezauważenie umieszczają je na komputerze użytkownika. Legalne programy do zdalnej administracji różnią się od trojanów typu backdoor do zdalnej administracji. Trojanzy potrafią niezależnie spenetrować system i zainstalować się; legalne programy nie potrafią tego.

Server-FTP	Serwery FTP	Działają jak serwery FTP. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu FTP.
Server-Proxy	Serwery proxy	Działają jak serwery proxy. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
Server-Telnet	Serwery Telnet	Działają jak serwery Telnet. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu Telnet.
Server-Web	Serwery sieciowe	Działają jak serwery sieciowe. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu HTTP.
RiskTool	Narzędzia wykorzystywane do pracy na lokalnym komputerze	Umożliwiają one użytkownikowi korzystanie z dodatkowych funkcji podczas jego pracy na komputerze. Narzędzia te pozwalają użytkownikowi ukryć pliki lub okna uruchomionych aplikacji i zakończyć aktywne procesy.
NetTool	Narzędzia sieciowe	Umożliwiają użytkownikowi korzystanie z dodatkowych funkcji podczas pracy z innymi komputerami w sieci. Posiadają one także możliwość ich ponownego uruchomienia, wykrywania otwartych portów oraz uruchamiania aplikacji zainstalowanych na komputerach.
Client-P2P	Klienty sieciowe P2P	Pozwalają pracować w sieciach peer-to-peer. Mogą być wykorzystywane przez hakerów do rozprzestrzeniania szkodliwego oprogramowania.
Client-SMTP	Klienty SMTP	Wysyłają wiadomości e-mail bez wiedzy użytkownika. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
WebToolbar	Paski narzędzi w przeglądarkach internetowych	Dodają one paski narzędzi w interfejsie innych aplikacji umożliwiające korzystanie z wyszukiwarek internetowych.
FraudTool	Pseudo-programy	Podają się za inne programy. Na przykład, istnieją fałszywe programy antywirusowe, które wyświetlają wiadomości o wykryciu szkodliwego oprogramowania. W rzeczywistości nie skanują ani nie leczą niczego.

- Wykrywaj pozostałe programy, które mogą zostać wykorzystane przez przestępców do uszkodzenia komputera lub danych prywatnych 

Podkategoria: legalne oprogramowanie, które może zostać wykorzystane przez cyberprzestępców do uszkodzenia komputera i prywatnych danych.

Poziom zagrożenia: średni

Wiele z tych programów to nieszkodliwe oprogramowanie, z którego korzysta wielu użytkowników. Do tych programów zaliczają się: klienty IRC, auto-dialery, programy pobierające pliki, monitory aktywności systemu komputerowego, narzędzia do haseł, serwery usług FTP, HTTP i Telnet.

Jednakże, jeśli haker uzyska dostęp do tego typu programów lub jeśli zainstaluje te programy na komputerze użytkownika, to niektóre z ich funkcji mogą zostać użyte do naruszenia ochrony.

Aplikacje te mają różne funkcje; ich typy zostały opisane w poniższej tabeli.

Typ	Nazwa	Opis
Client-IRC	Klienty czatów internetowych	Użytkownicy instalują programy tego typu, aby móc rozmawiać z innymi w czasie rzeczywistym. Hakerzy używają ich do rozsyłania szkodliwych programów.
Dialer	Auto-dialery	Mogą nawiązywać połączenie telefoniczne za pośrednictwem modemu w trybie ukrycia.
Downloader	Programy do pobierania	Mogą pobierać pliki ze stron internetowych w trybie ukrycia.
Monitor	Programy do monitorowania	Umożliwiają monitorowanie aktywności na komputerze, na którym są zainstalowane (sprawdzają, które aplikacje są aktywne i w jaki sposób wymieniają dane z aplikacjami zainstalowanymi na innych komputerach).
PSWTool	Programy do przywracania haseł	Umożliwiają przeglądanie i przywracanie zapomnianych haseł. Hakerzy umieszczają je na komputerze w tym samym celu, w sposób niezauważalny dla użytkownika.
RemoteAdmin	Programy do zdalnej administracji	Są używane przez administratorów systemów. Programy te pozwalają uzyskać dostęp do interfejsu zdalnego komputera w celu jego monitorowania i zarządzania. W tym właśnie celu hakerzy niezauważenie umieszczają je na komputerze użytkownika. Legalne programy do zdalnej administracji różnią się od trojanów typu backdoor do zdalnej administracji. Trojanzy potrafią niezależnie spenetrować system i zainstalować się; legalne programy nie potrafią tego.

Server-FTP	Serwery FTP	Działają jak serwery FTP. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu FTP.
Server-Proxy	Serwery proxy	Działają jak serwery proxy. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
Server-Telnet	Serwery Telnet	Działają jak serwery Telnet. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu Telnet.
Server-Web	Serwery sieciowe	Działają jak serwery sieciowe. Hakerzy instalują je na komputerach użytkowników w celu uzyskania do nich zdalnego dostępu przy użyciu protokołu HTTP.
RiskTool	Narzędzia wykorzystywane do pracy na lokalnym komputerze	Umożliwiają one użytkownikowi korzystanie z dodatkowych funkcji podczas jego pracy na komputerze. Narzędzia te pozwalają użytkownikowi ukryć pliki lub okna uruchomionych aplikacji i zakończyć aktywne procesy.
NetTool	Narzędzia sieciowe	Umożliwiają użytkownikowi korzystanie z dodatkowych funkcji podczas pracy z innymi komputerami w sieci. Posiadają one także możliwość ich ponownego uruchomienia, wykrywania otwartych portów oraz uruchamiania aplikacji zainstalowanych na komputerach.
Client-P2P	Klienty sieciowe P2P	Pozwalają pracować w sieciach peer-to-peer. Mogą być wykorzystywane przez hakerów do rozprzestrzeniania szkodliwego oprogramowania.
Client-SMTP	Klienty SMTP	Wysyłają wiadomości e-mail bez wiedzy użytkownika. Hakerzy instalują je na komputerze użytkownika w celu wysyłania spamu w jego imieniu.
WebToolbar	Paski narzędzi w przeglądarkach internetowych	Dodają one paski narzędzi w interfejsie innych aplikacji umożliwiające korzystanie z wyszukiwarek internetowych.
FraudTool	Pseudo-programy	Podają się za inne programy. Na przykład, istnieją fałszywe programy antywirusowe, które wyświetlają wiadomości o wykryciu szkodliwego oprogramowania. W rzeczywistości nie skanują ani nie leczą niczego.

- [Obiekty spakowane, których archiwizacja może być używana do ochrony szkodliwego kodu](#) 

Kaspersky Endpoint Security skanuje skompresowane obiekty i moduł wypakowujący znajdujące się w archiwach SFX (samorozpakowujących się).

Aby ukryć szkodliwe programy przed antywirusami, hakerzy archiwizują je przy pomocy dedykowanych narzędzi pakujących lub tworzą wielokrotnie spakowane obiekty.

Analitycy wirusów Kaspersky zidentyfikowali narzędzia pakujące najpopularniejsze wśród hakerów.

Jeśli Kaspersky Endpoint Security wykryje jeden z tych pakierów w pliku, plik ten najprawdopodobniej zawiera szkodliwą aplikację lub aplikację, która może zostać użyta przez cyberprzestępców do uszkodzenia komputera lub danych osobistych.

Kaspersky Endpoint Security wyróżnia następujące typy programów:

- *Spakowane pliki, które mogą wyrządzić szkody* – wykorzystywane do pakowania szkodliwego oprogramowania, takiego jak wirusy, robaki i trojany.
- *Pliki wielokrotnie spakowane (średni poziom zagrożenia)* – obiekt został spakowany trzy razy przez jedno lub więcej narzędzi pakujących.

- [Obiekty spakowane wielokrotnie](#) 

Kaspersky Endpoint Security skanuje skompresowane obiekty i moduł wypakowujący znajdujące się w archiwach SFX (samorozpakowujących się).

Aby ukryć szkodliwe programy przed antywirusami, hakerzy archiwizują je przy pomocy dedykowanych narzędzi pakujących lub tworzą wielokrotnie spakowane obiekty.

Analitycy wirusów Kaspersky zidentyfikowali narzędzia pakujące najpopularniejsze wśród hakerów.

Jeśli Kaspersky Endpoint Security wykryje jeden z tych pakierów w pliku, plik ten najprawdopodobniej zawiera szkodliwą aplikację lub aplikację, która może zostać użyta przez cyberprzestępców do uszkodzenia komputera lub danych osobistych.

Kaspersky Endpoint Security wyróżnia następujące typy programów:

- *Spakowane pliki, które mogą wyrządzić szkody* – wykorzystywane do pakowania szkodliwego oprogramowania, takiego jak wirusy, robaki i trojany.
- *Pliki wielokrotnie spakowane (średni poziom zagrożenia)* – obiekt został spakowany trzy razy przez jedno lub więcej narzędzi pakujących.

Wykluczenia

Ta tabela zawiera informacje o wykluczeniach ze skanowania.

Możliwe jest wykluczenie obiektów ze skanowania przy użyciu następujących metod:

- Określ ścieżkę do pliku lub folderu.

- Wprowadź sumę kontrolną obiektu.
- Użyj masek:
 - Znak ***** (gwiazdka), który zastępuje dowolny zestaw znaków, za wyjątkiem znaków: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:**.txt** będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderach na dysku C:, ale nie w podfolderach.
 - Dwa występujące po sobie znaki ***** zastępują dowolny zestaw znaków (w tym pusty zestaw) w nazwie pliku lub folderu, w tym znaki: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:\Folder***.txt** będzie zawierała wszystkie ścieżki do plików z rozszerzeniem TXT, znajdujących się w folderze o nazwie **Folder** i w jego podfolderach. Maskę musi zawierać przynajmniej jeden poziom zagnieżdżenia. Maskę **C:***.txt** nie jest ważną maską.
 - Znak **?** (znak zapytania), który zastępuje dowolny pojedynczy znak, za wyjątkiem znaków: **** i **/** (separatory nazw plików i folderów w ścieżkach dostępu do plików i folderów). Na przykład, maska **C:\Folder\???.txt** będzie zawierała ścieżki do wszystkich plików znajdujących się w folderze o nazwie **Folder**, które posiadają rozszerzenie TXT i nazwę składającą się z trzech znaków.
 - Wprowadź nazwę typu obiektu zgodnie z klasyfikacją [Encyklopedii Kaspersky](#) (na przykład: **Email-Worm**, **Rootkit** lub **RemoteAdmin**). Możesz użyć masek ze znakiem **?** (zastępuje dowolny pojedynczy znak) oraz znak ***** (zastępuje dowolną liczbę znaków). Na przykład, jeśli określona jest maska **Client***, Kaspersky Endpoint Security wyklucza obiekty **Client-IRC**, **Client-P2P** i **Client-SMTP** ze skanowania.

Zaufane aplikacje

Ta tabela wyświetla zaufane aplikacje, których aktywność nie jest monitorowana przez Kaspersky Endpoint Security w trakcie działania.

Komponent Kontrola aplikacji reguluje uruchamianie każdej aplikacji niezależnie od tego, czy aplikacja znajduje się w tabeli zaufanych aplikacji.

Przeniesienie wartości podczas dziedziczenia

(dostępny tylko w Kaspersky Security Center Console)

To powoduje scalenie listy wykluczeń ze skanowania i zaufanych aplikacji w zasadach nadrzędnych i potomnych programu Kaspersky Security Center. Aby scalić listy, zasada potomna musi być skonfigurowana do dziedziczenia ustawień zasady nadrzędnej programu Kaspersky Security Center.

Jeśli pole jest zaznaczone, w zasadach potomnych wyświetlane są elementy listy z zasady nadrzędnej Kaspersky Security Center. W ten sposób możesz, na przykład, utworzyć skonsolidowaną listę zaufanych aplikacji dla całej organizacji.

Dziedziczone elementy listy w zasadzie potomnej nie mogą zostać usunięte ani edytowane. Elementy na liście wykluczeń ze skanowania oraz lista zaufanych aplikacji, które są scalone podczas dziedziczenia, mogą zostać usunięte i edytowane tylko w zasadzie nadrzędnej. Możesz dodawać, edytować lub usuwać elementy z list w zasadach niższego poziomu.

Jeśli elementy na listach zasady potomnej i nadrzędnej pasują do siebie, te elementy są wyświetlane jak podobne elementy zasady nadrzędnej.

Jeśli pole nie zostało zaznaczone, elementy z list nie są scalane podczas dziedziczenia ustawień zasad programu Kaspersky Security Center.

Zezwól na korzystanie z lokalnych wykluczeń / Zezwól na

Lokalne wykluczenia i lokalne zaufane aplikacje (lokalna strefa zaufana) – lista obiektów i aplikacji zdefiniowana przez użytkownika w Kaspersky Endpoint Security dla określonego komputera. Kaspersky Endpoint Security nie monitoruje obiektów i aplikacji z lokalnej strefy zaufanej. W ten sposób użytkownicy mogą [utworzyć swoje własne lokalne listy wykluczeń i zaufanych aplikacji](#) jako dodatek do ogólnej strefy zaufanej w zasadzie.

<p>korzystanie z lokalnych zaufanych aplikacji</p> <p>(dostępny tylko w Kaspersky Security Center Console)</p>	<p>Jeśli pole jest zaznaczone, użytkownik może utworzyć lokalną listę wykluczeń skanowania i lokalnej listy zaufanej aplikacji. Administrator może użyć Kaspersky Security Center do przeglądania, dodawania, edytowania lub usuwania elementów listy we właściwościach komputera.</p> <p>Jeśli pole jest odznaczone, użytkownik może uzyskać dostęp tylko do ogólnych list wykluczeń ze skanowania i zaufanych aplikacji, wygenerowanych w zasadzie. Jeśli lokalne listy zostały wygenerowane, po wyłączeniu tej funkcjonalności program Kaspersky Endpoint Security kontynuuje wykluczenie listy obiektów ze skanowania.</p>
<p>Magazyn zaufanych certyfikatów systemowych</p>	<p>Jeśli wybrano jeden z zaufanych magazynów certyfikatów systemowych, Kaspersky Endpoint Security wyklucza ze skanowania aplikacje posiadające zaufany podpis cyfrowy. Kaspersky Endpoint Security automatycznie przypisze takie aplikacje do grupy <i>Zaufane</i>.</p> <p>Jeśli wybrano Nie używaj, Kaspersky Endpoint Security skanuje aplikacje niezależnie od tego, czy posiadają podpis cyfrowy. Kaspersky Endpoint Security umieszcza aplikację w grupie zaufania, w zależności od poziomu zagrożenia, jakie ta aplikacja może stwarzać dla komputera.</p>

Ustawienia aplikacji

Możesz skonfigurować następujące ogólne ustawienia aplikacji:

- Tryb działania
- Autoochrona
- Wydajność
- Informacje debugowania
- Stan komputera po zastosowaniu ustawień

Ustawienia aplikacji

Parametr	Opis
<p>Włącz Kaspersky Endpoint Security for Windows podczas uruchamiania komputera</p>	<p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security uruchamia się po załadowaniu systemu operacyjnego, chroniąc komputer w trakcie całej sesji.</p> <p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie uruchamia się po załadowaniu systemu operacyjnego dopóki użytkownik nie włączy go ręcznie. Ochrona komputera jest wyłączona, a dane użytkownika mogą być narażone na zagrożenia.</p>
<p>Użyj technologii zaawansowanego leczenia (wymaga znacznych zasobów komputera)</p>	<p>Jeśli pole jest zaznaczone, w momencie wykrycia szkodliwej aktywności w systemie operacyjnym na ekranie zostanie wyświetlony odpowiedni komunikat. W tym komunikacie Kaspersky Endpoint Security zaoferuje użytkownikowi przeprowadzenie zaawansowanego leczenia komputera. Jeśli użytkownik wyrazi zgodę na zastosowanie tej procedury, Kaspersky Endpoint Security zneutralizuje to zagrożenie. Po zakończeniu procedury zaawansowanego leczenia, Kaspersky Endpoint Security uruchamia ponownie komputer. Technologia zaawansowanego leczenia wykorzystuje dużą ilość zasobów komputera, co może spowolnić inne aplikacje.</p>

	<p>Jeśli aplikacja jest w trakcie wykrywania aktywnej infekcji, niektóre funkcje systemu mogą być niedostępne. Dostępność systemu operacyjnego jest przywracana, gdy Zaawansowane leczenie zostanie zakończone, a komputer zostanie uruchomiony ponownie.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Jeśli program Kaspersky Endpoint Security jest zainstalowany na komputerze działającym pod kontrolą systemu Windows przeznaczonego dla serwerów, Kaspersky Endpoint Security nie wyświetli komunikatu. Dlatego użytkownik nie może wybrać działania wyleczenia aktywnego zagrożenia. Aby wyleczyć zagrożenie, musisz włączyć technologię zaawansowanego leczenia w ustawieniach aplikacji oraz natychmiast włączyć Zaawansowane leczenie w ustawieniach zadania <i>Skanowanie antywirusowe</i>. Następnie musisz uruchomić zadanie <i>Skanowanie antywirusowe</i>.</p> </div>
<p>Użyj Kaspersky Security Center jako serwera proxy do aktywacji <i>(dostępny tylko w Kaspersky Security Center Console)</i></p>	<p>Jeśli topole jest zaznaczone, Serwer administracyjny Kaspersky Security Center jest używany jako serwer proxy podczas aktywacji aplikacji.</p>
<p>Włącz Autoochronę</p>	<p>Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security uniemożliwia modyfikowanie i usuwanie plików aplikacji, procesów pamięci i wpisów w rejestrze systemowym.</p>
<p>Zezwól na zarządzanie ustawieniami Kaspersky Endpoint Security za pomocą aplikacji do zdalnego zarządzania</p>	<p>Jeśli pole zostanie zaznaczone, zaufane aplikacje do zdalnego zarządzania (takie, jak TeamViewer, LogMeln Pro i Remotely Anywhere) mogą zmodyfikować ustawienia Kaspersky Endpoint Security.</p> <p>Zabronione jest modyfikowanie ustawień Kaspersky Endpoint Security przez niezauwane aplikacje do zdalnej administracji nawet wtedy, gdy zaznaczone jest pole.</p>
<p>Włącz możliwość zewnętrznej kontroli usługi</p>	<p>Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security zezwala na zarządzanie usługami aplikacji ze zdalnego komputera. Przy próbie zdalnego zarządzania usługami aplikacji, na pasku zadań Microsoft Windows, nad ikoną aplikacji wyświetlane jest powiadomienie (chyba, że usługa powiadomień została wyłączona przez użytkownika).</p>
<p>Odrocz zaplanowane zadania podczas pracy na bateriach</p>	<p>Jeżeli pole jest zaznaczone, włączony będzie tryb oszczędzania energii. Kaspersky Endpoint Security odroczy zaplanowane zadania. W razie konieczności zadania skanowania i aktualizacji mogą zostać uruchomione ręcznie.</p>
<p>Współdziel zasoby z innymi aplikacjami</p>	<p>Podczas wykonywania zaplanowanych zadań możliwe jest zwiększenie obciążenia procesora i podsystemów dysku, co spowalnia działanie innych aplikacji.</p> <p>Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security wstrzymuje zaplanowane zadania, gdy wykryje zwiększone obciążenie procesora i zwalnia zasoby systemu operacyjnego dla aplikacji użytkownika.</p>
<p>Włącz zapisywanie</p>	<p>Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security zapisuje pliki zrzutu w momencie awarii.</p>

zrzutów pamięci	Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie zapisuje plików zrzutu. Aplikacja także usuwa istniejące pliki zrzutu z dysku twardego komputera.
Włącz ochronę zrzutów pamięci i plików śledzenia	<p>Jeśli pole jest zaznaczone, dostęp do plików zrzutów pamięci jest udzielany systemowemu administratorowi i lokalnemu administratorowi, jak również użytkownikowi, który włączył zapis zrzutów pamięci. Tylko systemowi bądź lokalni administratorzy mają dostęp do plików śledzenia.</p> <p>Jeśli pole jest odznaczone, żaden użytkownik nie ma dostępu do plików zrzutów pamięci i plików śledzenia.</p>
Stan komputera po zastosowaniu ustawień <i>(dostępny tylko w Kaspersky Security Center Console)</i>	Ustawienia wyświetlania stanów komputerów klienckich z zainstalowanym programem Kaspersky Endpoint Security w Web Console, gdy podczas stosowania profilu lub wykonywania zadania wystąpią błędy. Dostępne są stany: <i>OK, Ostrzeżenie i Krytyczny</i> .

Raporty i pliki danych

Raporty

W raportach zapisywane są informacje o działaniu każdego modułu programu Kaspersky Endpoint Security, zdarzeniach szyfrowania danych, wykonaniu każdego zadania skanowania, zadania aktualizacji oraz zadania sprawdzania integralności, a także o ogólnym działaniu aplikacji.

Raporty są przechowywane w folderze C:\ProgramData\Kaspersky Lab\KES\Report.

Kopia zapasowa

Kopia zapasowa przechowuje zapasowe kopie plików, które zostały usunięte lub zmodyfikowane podczas leczenia. *Kopia zapasowa* to kopia pliku utworzona przed wyleczeniem lub usunięciem pliku. Kopie zapasowe plików są przechowywane w specjalnym formacie i nie stanowią zagrożenia.

Kopie zapasowe plików są przechowywane w folderze C:\ProgramData\Kaspersky Lab\KES\QB.

Użytkownicy należący do grupy Administratorzy mają nadane pełne uprawnienie dostępu do tego folderu. Ograniczone uprawnienia dostępu do tego folderu są nadawane użytkownikom, których konto zostało użyte do zainstalowania Kaspersky Endpoint Security.

Kaspersky Endpoint Security nie oferuje możliwości skonfigurowania uprawnień dostępu użytkownika do kopii zapasowych plików.

Kwarantanna

Kwarantanna to specjalny lokalny magazyn na komputerze, na którym zainfekowane pliki lub pliki nie dające się wyleczyć zostają przeniesione do tego właśnie katalogu. Pliki poddane kwarantannie są przechowywane w postaci zaszyfrowanej i nie zagrażają bezpieczeństwu urządzenia. Kaspersky Endpoint Security używa Kwarantanny tylko podczas pracy z rozwiązaniami Kaspersky Sandbox i Kaspersky Endpoint Detection and Response Optimum. W innych przypadkach Kaspersky Endpoint Security umieszcza odpowiedni plik w Kopii zapasowej. Więcej informacji na temat zarządzania Kwarantanną jako częścią rozwiązań można znaleźć w *podręcznikach dotyczących [Kaspersky Sandbox](#) i [Kaspersky Endpoint Detection and Response Optimum](#)*.

Kwarantanna może być skonfigurowana tylko za pośrednictwem konsoli Web Console. Możesz także użyć konsoli Web Console do zarządzania obiektami poddanymi kwarantannie (przywróć, usuń, dodaj itd.). Możesz przywrócić obiekty lokalnie na komputerze przy użyciu [wiersza polecenia](#).

Kaspersky Endpoint Security używa konta systemowego (SYSTEM) do poddania plików kwarantannie.

Ustawienia raportów i plików danych

Parametr	Opis
Przechowuj raporty nie dłużej niż N dni	Jeśli pole jest zaznaczone, maksymalny czas przechowywania raportu jest ograniczony do zdefiniowanego przedziału czasu. Domyślnie maksymalny czas przechowywania raportów wynosi 30 dni. Po tym czasie Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy z pliku raportu.
Ogranicz rozmiar pliku raportu do N MB	Jeśli pole jest zaznaczone, maksymalny rozmiar pliku raportu jest ograniczony do zdefiniowanej wartości. Domyślnie maksymalny rozmiar pliku wynosi 1024 MB. Aby uniknąć przekroczenia maksymalnego rozmiaru pliku raportu, Kaspersky Endpoint Security automatycznie usuwa najstarsze wpisy z pliku raportu po osiągnięciu maksymalnego rozmiaru pliku raportu.
Przechowuj obiekty nie dłużej niż N dni	Jeśli pole jest zaznaczone, maksymalny czas przechowywania pliku jest ograniczony do zdefiniowanego przedziału czasu. Domyślnie maksymalny czas przechowywania plików wynosi 30 dni. Po minięciu zdefiniowanego czasu, Kaspersky Endpoint Security usunie najstarsze pliki z Kopii zapasowej.
Ogranicz rozmiar Kopii zapasowej do N MB	Jeśli pole jest zaznaczone, maksymalny rozmiar magazynu jest ograniczony do zdefiniowanej wartości. Domyślnie wynosi on 100 MB. Aby uniknąć przekroczenia maksymalnego rozmiaru magazynu, Kaspersky Endpoint Security automatycznie usuwa najstarsze pliki z magazynu po osiągnięciu maksymalnego rozmiaru magazynu.
Ogranicz rozmiar Kwarantanny do N MB <i>(dostępna tylko w Web Console)</i>	Maksymalny rozmiar Kwarantanny w MB. Na przykład, możesz ustawić maksymalny rozmiar Kwarantanny na 200 MB. Jeśli Kwarantanna osiągnie maksymalny rozmiar, Kaspersky Endpoint Security wyśle odpowiednie zdarzenie do Kaspersky Security Center i opublikuje zdarzenie w Dzienniku zdarzeń Windows. W międzyczasie aplikacja kontynuuje poddawanie nowych obiektów kwarantannie.
Powiadom, gdy miejsce w kwarantannie osiągnie N procent <i>(dostępna tylko w Web Console)</i>	Wartość progowa Kwarantanny. Na przykład, możesz ustawić wartość progową Kwarantanny na 50%. Jeśli Kwarantanna osiągnie wartość progową, Kaspersky Endpoint Security wyśle odpowiednie zdarzenie do Kaspersky Security Center i opublikuje zdarzenie w Dzienniku zdarzeń Windows. W międzyczasie aplikacja kontynuuje poddawanie nowych obiektów kwarantannie.
Przesyłanie danych do Serwera administracyjnego <i>(dostępny tylko w Kaspersky Security Center)</i>	Kategorie zdarzeń na komputerach klienckich, których informacje muszą być wysłane do Serwera administracyjnego.

Ustawienia sieci

Możliwe jest skonfigurowanie serwera proxy używanego do nawiązywania połączenia z internetem i aktualizowania antywirusowych baz danych, wybranie trybu monitorowania portu sieciowego oraz konfigurowania skanowań połączeń szyfrowanych.

Opcje sieciowe

Parametr	Opis
Ogranicz ruch dla połączeń taryfowych	<p>Jeśli to pole jest zaznaczone, aplikacja ogranicza ruch sieciowy, gdy połączenie internetowe jest limitowane. Kaspersky Endpoint Security identyfikuje mobilne połączenia internetowe jako taryfowe, natomiast połączenia Wi-Fi jako nietaryfowe.</p> <p>Uwzględnienie kosztów połączenia działa na komputerach z systemem Windows 8 lub nowszy.</p>
Wstrzykuj skrypt do ruchu sieciowego w celu interakcji ze stronami internetowymi	<p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security wstrzykuje skrypt interakcji ze stronami internetowymi do ruchu sieciowego. Ten skrypt zapewnia poprawne działanie komponentu Kontrola sieci. Skrypt włącza rejestrację zdarzeń Kontroli sieci. Bez tego skryptu nie możesz włączyć monitorowanie aktywności internetowej użytkownika.</p> <div style="background-color: #f8d7da; padding: 10px;"><p>Ekspert z Kaspersky zalecają wstrzyknięcie tego skryptu interakcji ze stronami internetowymi do ruchu sieciowego w celu zapewnienia poprawnego działania Kontroli sieci.</p></div>
Serwer proxy	<p>Ustawienia serwera proxy używanego do łączenia z internetem użytkowników komputerów klienckich. Program Kaspersky Endpoint Security używa tych ustawień dla pewnych komponentów ochrony, jak również do uaktualniania baz danych i modułów aplikacji.</p> <p>Do automatycznej konfiguracji serwera proxy Kaspersky Endpoint Security używa protokołu WPAD (Web Proxy Auto-Discovery Protocol). Jeśli adres IP serwera proxy nie może zostać określony przy pomocy tego protokołu, Kaspersky Endpoint Security użyje adresu serwera proxy określonego w ustawieniach przeglądarki Microsoft Internet Explorer.</p>
Nie wykorzystuj serwera proxy dla adresów lokalnych	<p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security nie korzysta z serwera proxy przy wykonywaniu aktualizacji z foldera współdzielonego.</p>
Monitorowane porty	<p>Monitoruj wszystkie porty sieciowe. W tym trybie monitorowania portów sieciowych składniki ochrony (Ochrona plików, Ochrona WWW, Ochrona poczty) monitorują strumień danych przesyłane przez dowolne otwarte porty sieciowe komputera.</p> <p>Monitoruj tylko wybrane porty sieciowe. W tym trybie monitorowania portu sieciowego składniki ochrony monitorują wybrane porty komputera i aktywność sieciową wybranych aplikacji. Lista portów sieciowych używanych zazwyczaj do przesyłania wiadomości e-mail i ruchu internetowego jest konfigurowana zgodnie z zaleceniami ekspertów z Kaspersky.</p> <p>Monitoruj wszystkie porty dla aplikacji z listy zalecanej przez Kaspersky. To powoduje używanie predefiniowanej listy aplikacji, których porty sieciowe są monitorowane przez Kaspersky Endpoint Security. Na przykład, ta lista zawiera Google Chrome, Adobe Reader, Java i inne aplikacje.</p>

Monitoruj wszystkie porty dla określonych aplikacji. To powoduje używanie listy aplikacji, których porty sieciowe są monitorowane przez Kaspersky Endpoint Security.

Skanowanie połączeń szyfrowanych

Kaspersky Endpoint Security skanuje zaszyfrowany ruch sieciowy przesyłany za pośrednictwem następujących protokołów:

- SSL 3.0.
- TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

Kaspersky Endpoint Security obsługuje następujące tryby skanowania połączenia szyfrowanego:

- **Nie skanuj połączeń szyfrowanych** Kaspersky Endpoint Security nie będzie miał dostępu do zawartości stron internetowych, których adresy zaczynają się od <https://>.
- **Skanuj połączenia szyfrowane po zgłoszeniach od składników ochrony.** Kaspersky Endpoint Security będzie skanował zaszyfrowany ruch sieciowy tylko na żądanie składników: Ochrona plików, Ochrona poczty i Ochrona WWW.
- **Zawsze skanuj połączenia szyfrowane** Kaspersky Endpoint Security będzie skanował zaszyfrowany ruch sieciowy nawet wtedy, gdy składniki ochrony są wyłączone.

Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych, które zostały nawiązane przez [zaufane aplikacje, dla których skanowanie ruchu sieciowego jest wyłączone](#). Kaspersky Endpoint Security nie skanuje połączeń szyfrowanych z predefiniowanej listy zaufanych stron internetowych. Predefiniowana lista zaufanych stron internetowych jest tworzona przez ekspertów Kaspersky. Ta lista jest aktualizowana o antywirusowe bazy danych aplikacji. Predefiniowaną listę zaufanych stron internetowych możesz przejrzeć tylko w interfejsie Kaspersky Endpoint Security. Listy nie można przejrzeć w Kaspersky Security Center Console.

Podczas odwiedzania domeny z niezaufanym certyfikatem

- **Zezwól.** Jeśli ta opcja jest zaznaczona, podczas odwiedzania domeny z niezaufanym certyfikatem, Kaspersky Endpoint Security zezwoli na połączenie sieciowe.

Podczas otwierania domeny z niezaufanym certyfikatem w przeglądarce, Kaspersky Endpoint Security wyświetla stronę HTML pokazującą ostrzeżenie i powód, z jakiego odwiedzenie tej domeny nie jest zalecane. Użytkownik może kliknąć odnośnik ze strony ostrzegającej HTML, aby uzyskać dostęp do żądanego zasobu internetowego. Po kliknięciu tego odnośnika, w ciągu następnej godziny Kaspersky Endpoint Security nie wyświetli ostrzeżeń o niezaufanym certyfikacie podczas odwiedzania innych zasobów na tej samej domenie.

- **Blokuj połączenie.** Jeśli ta opcja jest zaznaczona, podczas odwiedzania domeny z niezaufanym certyfikatem, Kaspersky Endpoint Security blokuje połączenie sieciowe.

Podczas otwierania domeny z niezaufanym certyfikatem w przeglądarce, Kaspersky Endpoint Security wyświetla stronę HTML pokazującą powód zablokowania tej domeny.

W przypadku wystąpienia błędów skanowania połączenia szyfrowanego

- **Blokuj połączenie.** Jeśli ten element jest wybrany, gdy wystąpi błąd skanowania połączenia szyfrowanego, Kaspersky Endpoint Security zablokuje połączenie sieciowe.
- **Dodaj domenę do wykluczeń.** Jeśli ten element jest wybrany, gdy wystąpi błąd skanowania połączenia szyfrowanego, Kaspersky Endpoint Security doda domenę, w

	<p>której wystąpił błąd, do listy domen z błędami skanowania i nie będzie monitorował szyfrowanego ruchu sieciowego, gdy ta domena będzie odwiedzana. Możesz przejrzeć listę domen z błędami skanowania połączeń szyfrowanych tylko w lokalnym interfejsie aplikacji. Aby wyczyścić zawartość listy, należy wybrać Zablokuj połączenie.</p>
<p>Zablokuj połączenia SSL 2.0 (zalecane)</p>	<p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security zablokuje połączenia sieciowe nawiązane po protokole SSL 2.0.</p> <p>Jeśli pole jest odznaczone, Kaspersky Endpoint Security nie zablokuje połączeń sieciowych nawiązanych po protokole SSL 2.0 i nie będzie monitorował ruchu sieciowego przesyłanego przez te połączenia.</p>
<p>Deszyfruj szyfrowane połączenia ze stronami internetowymi używającymi certyfikatów EV</p>	<p>Certyfikaty EV (Extended Validation Certificates) potwierdzają autentyczność stron internetowych i zwiększają ochronę połączenia. Przeglądarki używają ikony kłódki w paskach adresu, aby pokazać, że strona internetowa posiada certyfikat EV. W przeglądarkach pasek adresu może być częściowo lub całkowicie oznaczony na zielono.</p> <p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security deszyfruje i monitoruje połączenia szyfrowane ze stronami internetowymi, które używają certyfikatu EV.</p> <p>Jeśli pole jest odznaczone, Kaspersky Endpoint Security nie ma dostępu do zawartości ruchu sieciowego HTTPS. Z tego powodu aplikacja monitoruje ruch sieciowy HTTPS tylko w oparciu o adres strony internetowej, na przykład: <code>https://google.com</code>.</p> <p>Jeśli otwierasz stronę internetową z certyfikatem EV po raz pierwszy, zaszyfrowane połączenie zostanie odszyfrowane niezależnie od tego, czy pole jest zaznaczone.</p>
<p>Zaufane adresy</p>	<p>To powoduje użycie listy adresów internetowych, dla których Kaspersky Endpoint Security nie skanuje połączeń sieciowych. Możesz wprowadzić nazwę domeny lub adres IP. Kaspersky Endpoint Security obsługuje znak <code>*</code> do wprowadzenia maski w nazwie domeny.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security nie obsługuje masek dla adresów IP. W lokalnym interfejsie aplikacji możesz wprowadzić zakres adresów IP (na przykład: 198.51.100.0/24). Zakresu adresów IP nie możesz wprowadzić w konsoli Kaspersky Security Center.</p> </div> <p>Na przykład:</p> <ul style="list-style-type: none"> <code>domain.com</code> – wpis jest częścią następujących adresów: <code>https://domain.com</code>, <code>https://www.domain.com</code>, <code>https://domain.com/page123</code>. Wpis nie jest częścią poddomen (na przykład: <code>subdomain.domain.com</code>). <code>subdomain.domain.com</code> – wpis jest częścią następujących adresów: <code>https://subdomain.domain.com</code>, <code>https://subdomain.domain.com/page123</code>. Wpis nie jest częścią domeny <code>domain.com</code>. <code>*.domain.com</code> – wpis jest częścią następujących adresów: <code>https://movies.domain.com</code>, <code>https://images.domain.com/page123</code>. Wpis nie jest częścią domeny <code>domain.com</code>.
<p>Zaufane aplikacje</p>	<p>Lista aplikacji, których aktywność nie jest monitorowana przez Kaspersky Endpoint Security w trakcie działania. Możesz wybrać typy aktywności aplikacji, których Kaspersky Endpoint Security nie będzie monitorował (na przykład, żeby nie skanował ruchu sieciowego). Podczas wprowadzania maski Kaspersky Endpoint Security obsługuje zmienne środowiskowe oraz znaki <code>*</code> i <code>?</code>.</p>
<p>Skanuj</p>	<p>Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security skanuje zaszyfrowany ruch</p>

bezpieczny ruch sieciowy w aplikacjach Mozilla

(dostępne tylko w interfejsie Kaspersky Endpoint Security)

sieciowy w przeglądarce Mozilla Firefox oraz w kliencie poczty Thunderbird. Dostęp do niektórych stron internetowych za pośrednictwem protokołu HTTPS może zostać zablokowany.

Aby skanować ruch sieciowy w przeglądarce Mozilla Firefox i kliencie poczty Thunderbird, musisz [włączyć Skanowanie połączeń szyfrowanych](#). Jeśli Skanowanie połączeń szyfrowanych jest wyłączone, Kaspersky Endpoint Security nie skanuje ruchu sieciowego w przeglądarce Mozilla Firefox oraz w kliencie poczty Thunderbird.

Kaspersky Endpoint Security używa certyfikatu głównego Kaspersky do odszyfrowania i analizowania zaszyfrowanego ruchu sieciowego. Możesz wybrać magazyn certyfikatów, który będzie zawierał certyfikat główny Kaspersky.

- **Użyj magazynu certyfikatów systemu Windows.** Certyfikat główny Kaspersky zostanie dodany do tego magazynu podczas instalacji Kaspersky Endpoint Security.
- **Użyj magazynu certyfikatów Mozilla.** Mozilla Firefox i Thunderbird używają swoich własnych magazynów certyfikatów. Jeśli wybrano magazyn certyfikatów aplikacji Mozilla, powinieneś ręcznie dodać certyfikat główny Kaspersky do tego magazynu z poziomu właściwości przeglądarki.

Interfejs

Możesz skonfigurować ustawienia interfejsu aplikacji.

Ustawienia interfejsu

Parametr	Opis
Interakcja z użytkownikiem (dostępny tylko w Kaspersky Security Center Console)	<p>Z uproszczonym interfejsem. Na komputerze klienckim okno główne aplikacji jest niedostępne, a dostępna jest tylko ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić ograniczoną liczbę operacji na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji.</p> <p>Z pełnym interfejsem. Na komputerze klienckim dostępne są: okno główne Kaspersky Endpoint Security oraz ikona w obszarze powiadomień systemu Windows. W menu kontekstowym ikony użytkownik może przeprowadzić operacje na Kaspersky Endpoint Security. Kaspersky Endpoint Security wyświetli także powiadomienia nad ikoną aplikacji.</p> <p>Ukryj sekcję Monitor aktywności aplikacji. Na komputerze klienckim, w oknie głównym Kaspersky Endpoint Security przycisk Monitor aktywności aplikacji jest niedostępny. <i>Monitor aktywności aplikacji</i> to narzędzie służące do wyświetlania informacji o aktywności aplikacji na komputerze użytkownika w czasie rzeczywistym.</p> <p>Brak interfejsu. Na komputerze klienckim nie są wyświetlane żadne działania Kaspersky Endpoint Security. Ikona w obszarze powiadomień systemu Windows oraz powiadomienia nie są dostępne.</p>
Ustawienia powiadomień	Tabela z ustawieniami powiadomień o zdarzeniach o różnych poziomach istotności, które mogą wystąpić w trakcie działania modułu, zadania lub aplikacji. Kaspersky Endpoint Security wyświetla powiadomienia o tych zdarzeniach, wysyła je za pośrednictwem poczty elektronicznej lub zapisuje je w raporcie.
Ustawienia powiadomiania	Ustawienia serwera SMTP do dostarczania powiadomień o zdarzeniach zarejestrowanych podczas działania aplikacji.

przy użyciu e-mail	
Pokaż stan aplikacji w obszarze powiadomień	Kategorie zdarzeń aplikacji, które powodują, że ikona Kaspersky Endpoint Security zmienia się w obszarze powiadomień paska zadań systemu Microsoft Windows (🔒 lub 📧) i powoduje wyświetlanie wiadomości wyskakującej.
Powiadomienia o stanie lokalnych antywirusowych baz danych	Ustawienia powiadomień o przestarzałych antywirusowych bazach danych używanych przez aplikację.
Ochrona hasłem	<p>Jeśli przycisk przełącznika jest włączony, Kaspersky Endpoint Security pyta użytkownika o hasło, gdy użytkownik próbuje wykonać działanie, które jest w obrębie obszaru Ochrony hasłem. Obszar Ochrony hasłem obejmuje zabronione działania (takie jak wyłączenie składników ochrony) oraz konta użytkowników, do których stosowany jest obszar Ochrony hasłem.</p> <p>Po włączeniu Ochrony hasłem, Kaspersky Endpoint Security wyświetli pytanie o ustawienie hasła do wykonywania działań.</p>
Zasoby sieciowe pomocy technicznej <i>(dostępny tylko w Kaspersky Security Center Console)</i>	Lista odsyłaczy do zasobów sieciowych z informacjami o pomocy technicznej dla Kaspersky Endpoint Security. Dodane odnośniki będą wyświetlane w oknie Pomoc techniczna lokalnego interfejsu Kaspersky Endpoint Security zamiast standardowych odnośników.
Wiadomość do użytkownika <i>(dostępny tylko w Kaspersky Security Center Console)</i>	Wiadomość, która jest wyświetlana w oknie Pomoc techniczna lokalnego interfejsu Kaspersky Endpoint Security.

Zarządzaj ustawieniami

Możesz zapisać bieżące ustawienia Kaspersky Endpoint Security do pliku i użyć ich do szybkiego skonfigurowania aplikacji na innym komputerze. Możesz użyć pliku konfiguracyjnego podczas zdalnej instalacji aplikacji za pośrednictwem Kaspersky Security Center 12 z użyciem [pakietu instalacyjnego](#). Możesz przywrócić domyślne ustawienia w dowolnym momencie.

Ustawienia zarządzania konfiguracją aplikacji są dostępne tylko w interfejsie Kaspersky Endpoint Security.

Ustawienia zarządzania konfiguracją aplikacji

Ustawienia	Opis
Importuj	Wydobywanie ustawień aplikacji z pliku w formacie CFG i ich stosowanie.
Eksportuj	Zapisywanie bieżących ustawień aplikacji do pliku w formacie CFG.
Przywróć	W każdej chwili możesz przywrócić ustawienia zalecane przez firmę Kaspersky dla Endpoint Security. Po przywróceniu ustawień, poziom ochrony wszystkich modułów zostaje ustawiony na Zalecany .

Aktualizowanie baz danych i modułów aplikacji

Aktualizowanie baz danych i modułów aplikacji Kaspersky Endpoint Security zapewnia aktualną ochronę Twojego komputera. Codziennie na całym świecie pojawia się duża ilość nowych wirusów i innego typu szkodliwego oprogramowania. Bazy danych Kaspersky Endpoint Security zawierają informacje o zagrożeniach i sposoby ich neutralizowania. Aby szybko wykrywać zagrożenia, zalecamy regularnie aktualizować bazy danych i moduły aplikacji.

Regularne aktualizacje wymagają ważnej licencji na aplikację. Jeżeli nie ma bieżącej licencji, wówczas możliwe będzie wykonanie tylko jednej aktualizacji.

Głównym źródłem uaktualnień dla Kaspersky Endpoint Security są serwery aktualizacji firmy Kaspersky.

Aby możliwe było pobieranie pakietów aktualizacji z serwerów aktualizacji Kaspersky, komputer musi być podłączony do internetu. Domyślnie ustawienia połączenia internetowego są określone automatycznie. Jeśli korzystasz z serwera proxy, konieczne może być dostosowanie ustawień serwera proxy.

Uaktualnienia są pobierane po protokole HTTPS. Mogą także zostać pobrane po protokole HTTP, jeśli niemożliwe jest pobranie uaktualnień po protokole HTTPS.

Podczas procesu aktualizacji, na komputer są pobierane i instalowane następujące obiekty:

- Bazy danych programu Kaspersky Endpoint Security. Ochrona komputera jest zapewniana przy pomocy baz danych zawierających sygnatury wirusów i innych zagrożeń oraz informacje o sposobach ich neutralizacji. Moduły ochrony korzystają z tych informacji przy wyszukiwaniu i neutralizowaniu zainfekowanych plików na Twoim komputerze. Bazy danych są ciągle aktualizowane o wpisy nowych zagrożeń i metody ich zwalczania. Dlatego zalecamy regularne aktualizowanie baz danych.

Oprócz baz danych Kaspersky Endpoint Security aktualizowane są również sterowniki sieciowe, które umożliwiają modułom aplikacji przechwytywanie ruchu sieciowego.

- Moduły aplikacji. Oprócz baz danych aplikacji można także aktualizować jej moduły. Aktualizowanie modułów aplikacji likwiduje luki w Kaspersky Endpoint Security, dodaje nowe funkcje lub poprawia te istniejące.

Podczas aktualizacji moduły i bazy danych aplikacji znajdujące się na komputerze porównywane są z tymi aktualnymi, znajdującymi się w źródle uaktualnień. Jeśli Twoje bieżące bazy danych i moduły różnią się od najnowszych wersji, na Twoim komputerze zainstalowana zostanie brakująca część uaktualnień.

Pliki pomocy kontekstowej mogą być aktualizowane wraz z modułami aplikacji.

Jeśli bazy danych są bardzo stare, pakiet uaktualnień może być duży, co spowoduje zwiększony ruch internetowy (kilkadziesiąt MB).

Informacje o bieżącym stanie baz danych Kaspersky Endpoint Security jest wyświetlany w oknie głównym aplikacji lub w dymku, który jest wyświetlany po najechaniu kursorem na ikonę aplikacji w obszarze powiadomień.

Informacje o wynikach aktualizacji i wszystkich zdarzeniach zaistniałych podczas wykonywania zadania aktualizacji zapisywane są w [raporcie Kaspersky Endpoint Security](#).

Parametr	Opis
Tryb uruchamiania	<p>Automatycznie. W tym trybie Kaspersky Endpoint Security sprawdza źródło uaktualnień z określoną częstotliwością w poszukiwaniu nowych pakietów aktualizacji. Częstotliwość sprawdzania w poszukiwaniu pakietu uaktualnień może wzrastać podczas epidemii wirusów, a maleć w okresach względnie spokojnych. Po wykryciu nowego pakietu aktualizacji, Kaspersky Endpoint Security pobiera go i instaluje aktualizacje na komputerze.</p> <p>Ręcznie. Ten tryb uruchamiania zadania aktualizacji umożliwia ręczne uruchomienie zadania aktualizacji.</p> <p>Zgodnie z terminarzem. W tym trybie Kaspersky Endpoint Security uruchamia zadanie aktualizacji zgodnie z ustalonym terminarzem. Jeśli wybrano ten tryb uruchamiania, zadanie aktualizacji może zostać również uruchomione ręcznie.</p>
Uruchom pominięte zadania	<p>Jeśli pole to jest zaznaczone, Kaspersky Endpoint Security uruchamia pominięte zadanie aktualizacji kiedy tylko będzie to możliwe. Zadanie aktualizacji może zostać pominięte, na przykład, jeśli komputer był wyłączony w zaplanowanym czasie uruchomienia zadania aktualizacji.</p> <p>Jeśli pole nie jest zaznaczone, Kaspersky Endpoint Security nie uruchamia pominiętych zadań aktualizacji. Zamiast tego uruchomi następną aktualizację zgodnie z bieżącym terminarzem.</p>
Źródło aktualizacji	<p><i>Źródło uaktualnień</i> jest zasobem zawierającym uaktualnienia baz danych oraz modułów aplikacji Kaspersky Endpoint Security.</p> <p>Źródłami uaktualnień mogą być serwer Kaspersky Security Center, serwery aktualizacji Kaspersky i foldery lokalne lub sieciowe.</p> <p>Domyślna lista źródeł uaktualnień zawiera serwery aktualizacji Kaspersky Security Center i Kaspersky. Do listy można dodać inne źródło uaktualnień. Źródłem uaktualnień mogą być serwery HTTP/FTP oraz foldery współdzielone.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Kaspersky Endpoint Security nie obsługuje aktualizacji z serwerów HTTPS, chyba że są to serwery aktualizacji Kaspersky.</p> </div> <p>Jeżeli jako aktywne ustawiono kilka źródeł uaktualnień, Kaspersky Endpoint Security będzie podejmował próby nawiązywania połączenia z każdym z nich, poczynwszy od góry listy; uaktualnienia zostaną pobrane z pierwszego dostępnego źródła.</p>
Uruchom zadanie jako	<p>Domyślnie zadanie aktualizacji Kaspersky Endpoint Security jest uruchamiane z poziomu konta użytkownika, którego użyłeś do uruchomienia systemu operacyjnego. Jednakże program Kaspersky Endpoint Security może zostać zaktualizowany ze źródła uaktualnień, do którego użytkownik nie ma dostępu ze względu na brak wymaganych uprawnień (na przykład, z folderu współdzielonego, który zawiera pakiet uaktualnień) lub ze źródła uaktualnień, dla którego nie skonfigurowano autoryzacji na serwerze proxy. W ustawieniach programu Kaspersky Endpoint Security możesz wskazać użytkownika, który posiada takie uprawnienia, i skonfigurować uruchamianie aktualizacji Kaspersky Endpoint Security z poziomu konta tego użytkownika.</p>
Pobierz aktualizacje składników aplikacji	<p>Pole to włącza / wyłącza pobieranie aktualizacji modułów aplikacji i uaktualnień antywirusowej bazy danych.</p> <p>Jeśli to pole jest zaznaczone, Kaspersky Endpoint Security powiadomi użytkownika o dostępnych uaktualnieniach modułów aplikacji i uwzględni te uaktualnienia w pakiecie uaktualnień podczas wykonywania zadania aktualizacji. Sposób stosowania uaktualnień modułów aplikacji jest określany przez następujące ustawienia:</p> <ul style="list-style-type: none"> • Instaluj krytyczne i zatwierdzone aktualizacje. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security automatycznie instaluje krytyczne uaktualnienia, a także wszystkie inne uaktualnienia

	<p>modułów aplikacji po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center.</p> <ul style="list-style-type: none"> • Instaluj tylko zatwierdzone aktualizacje. Jeśli ta opcja jest zaznaczona, gdy uaktualnienia modułów aplikacji są dostępne, Kaspersky Endpoint Security instaluje je po zatwierdzeniu ich instalacji, lokalnie z poziomu interfejsu aplikacji lub po stronie Kaspersky Security Center. Ta opcja jest wybrana domyślnie. <p>Jeśli to pole nie zostanie zaznaczone, Kaspersky Endpoint Security nie powiadomi użytkownika o dostępnych uaktualnieniach modułów aplikacji i nie uwzględni tych uaktualnień w pakiecie uaktualnień podczas wykonywania zadania aktualizacji.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>Jeśli uaktualnienia modułów aplikacji wymagają przeczytanie i zaakceptowanie warunków Umowy licencyjnej, aplikacja zainstaluje uaktualnienia po zaakceptowaniu warunków Umowy licencyjnej.</p> </div> <p>Domyślnie pole to jest zaznaczone.</p>
<p>Kopiuj aktualizacje do folderu</p>	<p>Jeśli to pole wyboru jest zaznaczone, Kaspersky Endpoint Security kopiuje pakiet aktualizacji do udostępnionego folderu określonego w polu wyboru. Następnie pozostałe komputery w sieci LAN pobierają pakiet uaktualnień z tego folderu współdzielonego. Ogranicza to ruch internetowy, ponieważ pakiet uaktualnień jest pobierany jednorazowo. Domyślnie określono następujący folder: C:\ProgramData\Kaspersky Lab\KES\Update distribution\.</p>
<p>Serwer proxy dla aktualizacji <i>(dostępne tylko w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Ustawienia serwera proxy dla dostępu użytkowników komputerów klienckich do internetu w celu przeprowadzenia aktualizacji baz danych i modułów aplikacji.</p> <p>Do automatycznej konfiguracji serwera proxy Kaspersky Endpoint Security używa protokołu WPAD (Web Proxy Auto-Discovery Protocol). Jeśli adres IP serwera proxy nie może zostać określony przy pomocy tego protokołu, Kaspersky Endpoint Security użyje adresu serwera proxy określonego w ustawieniach przeglądarki Microsoft Internet Explorer.</p>
<p>Nie wykorzystuj serwera proxy dla adresów lokalnych <i>(dostępne tylko w interfejsie Kaspersky Endpoint Security)</i></p>	<p>Jeśli pole jest zaznaczone, Kaspersky Endpoint Security nie korzysta z serwera proxy przy wykonywaniu aktualizacji z foldera współdzielonego.</p>

Dodatek 2. Grupy zaufania aplikacji

Kaspersky Endpoint Security przydziela wszystkie aplikacje, które są uruchomione na komputerze, do grup zaufania. Aplikacje są przydzielane do grup zaufania w zależności od poziomu zagrożenia, jakie stanowią dla systemu operacyjnego.

Istnieją następujące grupy zaufania:

- **Zaufana.** Ta grupa zawiera aplikacje, dla których spełniono jeden lub kilka następujących warunków:
 - Aplikacje są cyfrowo podpisane przez zaufanych producentów.
 - Aplikacje znajdują się w bazie danych zaufanych aplikacji z Kaspersky Security Network.
 - Użytkownik umieścił aplikacje w grupie Zaufane.

Dla takich aplikacji nie ma zabronionych akcji.

- **Niskie ograniczenia.** Ta grupa zawiera aplikacje, dla których spełniono następujące warunki:
 - Aplikacje nie są cyfrowo podpisane przez zaufanych producentów.
 - Aplikacje nie znajdują się w bazie danych zaufanych aplikacji z Kaspersky Security Network.
 - Użytkownik umieścił aplikacje w grupie "Niskie ograniczenia".

Takie aplikacje mają minimalne ograniczenia dostępu do zasobów systemu operacyjnego.

- **Wysokie ograniczenia.** Ta grupa zawiera aplikacje, dla których spełniono następujące warunki:
 - Aplikacje nie są cyfrowo podpisane przez zaufanych producentów.
 - Aplikacje nie znajdują się w bazie danych zaufanych aplikacji z Kaspersky Security Network.
 - Użytkownik umieścił aplikacje w grupie Wysokie ograniczenia.

Takie aplikacje mają wysokie ograniczenia dostępu do zasobów systemu operacyjnego.

- **Niezaufane.** Ta grupa zawiera aplikacje, dla których spełniono następujące warunki:
 - Aplikacje nie są cyfrowo podpisane przez zaufanych producentów.
 - Aplikacje nie znajdują się w bazie danych zaufanych aplikacji z Kaspersky Security Network.
 - Użytkownik umieścił aplikacje w grupie Niezaufane.

Dla tych aplikacji wszystkie działania są zablokowane.

Dodatek 3. Rozszerzenia plików do szybkiego skanowania dysków wymiennych

com – plik wykonywalny aplikacji nie większy niż 64 KB

exe – plik wykonywalny samorozpakowującego się archiwum

sys – plik systemu Microsoft Windows

prg – dla programu dBase™, Clipper, Microsoft Visual FoxPro® lub WAVmaker

bin – plik binarny

bat – plik wsadowy

cmd – plik polecenia dla Microsoft Windows NT (podobny do pliku bat dla DOS), OS/2

dpl – skompresowana biblioteka Borland Delphi

dll – biblioteka dołączana dynamicznie

scr – ekran powitalny Microsoft Windows

cpl – moduł panelu kontrolującego Microsoft Windows

ocx – obiekt OLE Microsoft (Łączenie i osadzanie obiektów)

tsp – program działający w trybie podziału czasu

drv – sterownik urządzenia

vxd – sterownik urządzenia wirtualnego Microsoft Windows

pif – plik PIF

lnk – plik łącza Microsoft Windows

reg – plik klucza rejestru systemu Microsoft Windows

ini – plik konfiguracyjny, który zawiera dane konfiguracyjne dla Microsoft Windows, Windows NT i niektórych aplikacji

cla – plik klasy języka Java

vbs – skrypt Visual Basic®

vbe – rozszerzenie BIOS-u kart graficznych

js, jse – tekst źródłowy JavaScript

htm – dokument hipertekstowy

htt – nagłówek hipertekstowy Microsoft Windows

hta – program hipertekstowy dla Microsoft Internet Explorer®

asp – skrypt Active Server Pages

chm – skompilowany plik HTML

pht – plik HTML ze zintegrowanymi skryptami PHP

php – skrypt zintegrowany w plikach HTML

wsh – plik Microsoft Windows Script Host

wsf – skrypt Microsoft Windows

the – plik tapety pulpitu Microsoft Windows 95

hlp – plik pomocy w formacie Win Help

eml – wiadomość pocztowa Microsoft Outlook Express

nws – nowa wiadomość pocztowa Microsoft Outlook Express

msg – wiadomość pocztowa Microsoft Mail

plg – wiadomość pocztowa

mbx – zapisane wiadomości e-mail Microsoft Office Outlook

doc* – dokumenty Microsoft Office Word, takie jak: doc dla dokumentów Microsoft Office Word, docx dla dokumentów Microsoft Office Word 2007 z obsługą XML oraz docm dla dokumentów Microsoft Office Word 2007 z obsługą makr

dot* – szablony dokumentów Microsoft Office Word, takie jak: dot dla szablonów dokumentów Microsoft Office Word, dotx dla szablonów dokumentów Microsoft Office Word 2007, dotm dla szablonów dokumentów Microsoft Office Word 2007 z obsługą makr

fpm – program bazodanowy, plik startowy dla Microsoft Visual FoxPro

rtf – dokument Rich Text Format

shs – fragment Windows Shell Scrap Object Handler

dwg – baza danych programu AutoCAD®

msi – pakiet Microsoft Windows Installer

otm – projekt VBA dla Microsoft Office Outlook

pdf – dokument Adobe Acrobat

swf – obiekt pakietu Shockwave® Flash

jpg, jpeg – skompresowany format graficzny

emf – plik formatu Enhanced Metafile;

ico – plik ikony obiektu

ov? – pliki wykonywalne Microsoft Office Word

xl* – pliki i dokumenty Microsoft Office Excel, takie jak: xla dla rozszerzeń dla Microsoft Office Excel, xlc dla diagramów, xlt dla szablonów dokumentów,.xlsx dla skoroszytów Microsoft Office Excel 2007, xltm dla skoroszytów Microsoft Office Excel 2007 z obsługą makr, xlsb dla skoroszytów Microsoft Office Excel 2007 w formacie binarnym (nie XML), xltx dla szablonów Microsoft Office Excel 2007, xlsx dla szablonów Microsoft Office Excel 2007 z obsługą makr oraz xlam dla wtyczek Microsoft Office Excel 2007 z obsługą makr

pp* – pliki i dokumenty Microsoft Office PowerPoint®, takie jak: pps dla slajdów Microsoft Office PowerPoint, ppt dla prezentacji, pptx dla prezentacji Microsoft Office PowerPoint 2007, pptm dla prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, potx dla szablonów prezentacji Microsoft Office PowerPoint 2007, potm dla szablonów prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, ppsx dla pokazów slajdów Microsoft Office PowerPoint 2007, ppsm dla pokazów slajdów Microsoft Office PowerPoint 2007 z obsługą makr oraz ppam dla wtyczek Microsoft Office PowerPoint 2007 z obsługą makr

md* – pliki i dokumenty Microsoft Office Access®, takie jak: mda dla grup roboczych Microsoft Office Access oraz mdb dla baz danych

sldx – slajd Microsoft PowerPoint 2007

sldm – slajd Microsoft PowerPoint 2007 z obsługą makr

thmx – motyw Microsoft Office 2007

Dodatek 4. Typy plików dla filtra załączników modułu Ochrona poczty

Należy pamiętać, że rzeczywisty format pliku może nie odpowiadać jego rozszerzeniu.

Jeśli włączyłeś filtrowanie załączników w wiadomościach, komponent Ochrona poczty może zmieniać nazwy plików lub usuwać pliki z następującymi rozszerzeniami:

com – plik wykonywalny aplikacji nie większy niż 64 KB

exe – plik wykonywalny samorozpakowującego się archiwum

sys – plik systemu Microsoft Windows

prg – dla programu dBase™, Clipper, Microsoft Visual FoxPro® lub WAVmaker

bin – plik binarny

bat – plik wsadowy

cmd – plik polecenia dla Microsoft Windows NT (podobny do pliku bat dla DOS), OS/2

dpl – skompresowana biblioteka Borland Delphi

dll – biblioteka dołączana dynamicznie

scr – ekran powitalny Microsoft Windows

cpl – moduł panelu kontrolującego Microsoft Windows

ocx – obiekt OLE Microsoft (Łączenie i osadzanie obiektów)

tsp – program działający w trybie podziału czasu

drv – sterownik urządzenia

vxd – sterownik urządzenia wirtualnego Microsoft Windows

pif – plik PIF

lnk – plik łącza Microsoft Windows

reg – plik klucza rejestru systemu Microsoft Windows

ini – plik konfiguracyjny, który zawiera dane konfiguracyjne dla Microsoft Windows, Windows NT i niektórych aplikacji

cla – plik klasy języka Java

vbs – skrypt Visual Basic®

vbe – rozszerzenie BIOS-u kart graficznych

js, jse – tekst źródłowy JavaScript

htm – dokument hipertekstowy

htt – nagłówek hipertekstowy Microsoft Windows

hta – program hipertekstowy dla Microsoft Internet Explorer®

asp – skrypt Active Server Pages

chm – skompilowany plik HTML

pht – plik HTML ze zintegrowanymi skryptami PHP

php – skrypt zintegrowany w plikach HTML

wsh – plik Microsoft Windows Script Host

wsf – skrypt Microsoft Windows

the – plik tapety pulpitu Microsoft Windows 95

hlp – plik pomocy w formacie Win Help

eml – wiadomość pocztowa Microsoft Outlook Express

nws – nowa wiadomość pocztowa Microsoft Outlook Express

msg – wiadomość pocztowa Microsoft Mail

plg – wiadomość pocztowa

mbx – zapisane wiadomości e-mail Microsoft Office Outlook

doc* – dokumenty Microsoft Office Word, takie jak: doc dla dokumentów Microsoft Office Word, docx dla dokumentów Microsoft Office Word 2007 z obsługą XML oraz docm dla dokumentów Microsoft Office Word 2007 z obsługą makr

dot* – szablony dokumentów Microsoft Office Word, takie jak: dot dla szablonów dokumentów Microsoft Office Word, dotx dla szablonów dokumentów Microsoft Office Word 2007, dotm dla szablonów dokumentów Microsoft Office Word 2007 z obsługą makr

fpm – program bazodanowy, plik startowy dla Microsoft Visual FoxPro

rtf – dokument Rich Text Format

shs – fragment Windows Shell Scrap Object Handler

dwg – baza danych programu AutoCAD®

msi – pakiet Microsoft Windows Installer

otm – projekt VBA dla Microsoft Office Outlook

pdf – dokument Adobe Acrobat

swf – obiekt pakietu Shockwave® Flash

jpg, jpeg – skompresowany format graficzny

emf – plik formatu Enhanced Metafile;

ico – plik ikony obiektu

ov? – pliki wykonywalne Microsoft Office Word

xl* – pliki i dokumenty Microsoft Office Excel, takie jak: xla dla rozszerzeń dla Microsoft Office Excel, xlc dla diagramów, xlt dla szablonów dokumentów, xlsx dla skoroszytów Microsoft Office Excel 2007, xltm dla skoroszytów Microsoft Office Excel 2007 z obsługą makr, xlsb dla skoroszytów Microsoft Office Excel 2007 w formacie binarnym (nie XML), xltx dla szablonów Microsoft Office Excel 2007, xlsx dla szablonów Microsoft Office Excel 2007 z obsługą makr oraz xlam dla wtyczek Microsoft Office Excel 2007 z obsługą makr

pp* – pliki i dokumenty Microsoft Office PowerPoint®, takie jak: pps dla slajdów Microsoft Office PowerPoint, ppt dla prezentacji, pptx dla prezentacji Microsoft Office PowerPoint 2007, pptm dla prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, potx dla szablonów prezentacji Microsoft Office PowerPoint 2007, potm dla szablonów prezentacji Microsoft Office PowerPoint 2007 z obsługą makr, ppsx dla pokazów slajdów Microsoft Office PowerPoint 2007, ppsm dla pokazów slajdów Microsoft Office PowerPoint 2007 z obsługą makr oraz ppam dla wtyczek Microsoft Office PowerPoint 2007 z obsługą makr

md* – pliki i dokumenty Microsoft Office Access®, takie jak: mda dla grup roboczych Microsoft Office Access oraz mdb dla baz danych

sldx – slajd Microsoft PowerPoint 2007

sldm – slajd Microsoft PowerPoint 2007 z obsługą makr

thmx – motyw Microsoft Office 2007

Dodatek 5. Ustawienia sieci do interakcji z usługami zewnętrznymi

Kaspersky Endpoint Security używa następujących ustawień sieciowych do interakcji z usługami zewnętrznymi.

Ustawienia sieci

Adres	Opis
<p>activation-v2.kaspersky.com/activation-service/activation-service.svc</p> <p>Protokół: HTTPS</p> <p>Port: 443</p>	<p>Aktywowanie aplikacji</p>
<p>s00.upd.kaspersky.com</p> <p>s01.upd.kaspersky.com</p> <p>s02.upd.kaspersky.com</p> <p>s03.upd.kaspersky.com</p> <p>s04.upd.kaspersky.com</p> <p>s05.upd.kaspersky.com</p> <p>s06.upd.kaspersky.com</p> <p>s07.upd.kaspersky.com</p> <p>s08.upd.kaspersky.com</p> <p>s09.upd.kaspersky.com</p> <p>s10.upd.kaspersky.com</p> <p>s11.upd.kaspersky.com</p> <p>s12.upd.kaspersky.com</p> <p>s13.upd.kaspersky.com</p> <p>s14.upd.kaspersky.com</p> <p>s15.upd.kaspersky.com</p> <p>s16.upd.kaspersky.com</p> <p>s17.upd.kaspersky.com</p> <p>s18.upd.kaspersky.com</p> <p>s19.upd.kaspersky.com</p> <p>cm.k.kaspersky-labs.com</p> <p>Protokół: HTTPS</p> <p>Port: 443</p>	<p>Aktualizowanie baz danych i modułów aplikacji</p>
<p>downloads.upd.kaspersky.com</p> <p>Protokół: HTTPS</p> <p>Port: 443</p>	<ul style="list-style-type: none"> • Aktualizowanie baz danych i modułów aplikacji • Sprawdzenie, czy serwery Kaspersky są dostępne. Jeśli dostęp do serwerów za pomocą systemowego DNS nie jest możliwy, aplikacja użyje publicznego DNS. Jest to konieczne, by upewnić się, że antywirusowe bazy danych są aktualizowane i że poziom bezpieczeństwa komputera jest utrzymywany. Kaspersky Endpoint Security używa

poniższej listy publicznych serwerów DNS w następującej kolejności:

1. Google Public DNS (8.8.8.8).
2. Cloudflare DNS (1.1.1.1).
3. Alibaba Cloud DNS (223.6.6.6).
4. Quad9 DNS (9.9.9.9).
5. CleanBrowsing (185.228.168.168).

Żądania wysyłane przez aplikację mogą zawierać adresy domen i publiczny adres IP użytkownika, ponieważ aplikacja nawiązuje połączenie TCP/UDP z serwerem DNS. Te informacje są niezbędne na przykład do walidacji certyfikatu zasobu sieciowego podczas korzystania z protokołu HTTPS. Jeśli Kaspersky Endpoint Security korzysta z publicznego serwera DNS, przetwarzanie danych jest regulowane przez politykę prywatności odpowiedniej usługi. Jeśli chcesz uniemożliwić Kaspersky Endpoint Security korzystanie z publicznego serwera DNS, skontaktuj się z działem pomocy technicznej w celu uzyskania prywatnej poprawki.

touch.kaspersky.com

Protokół: HTTP

- Odbieranie zaufanego czasu sprawdzania okresu ważności certyfikatu (połączenie TLS).
- Ostrzeżenie dotyczące odmowy dostępu do zasobu sieciowego w przeglądarce (Ochrona WWW i Kontrola sieci)

<p>p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com</p> <p>Protokół: HTTP</p> <p>Port: 80</p>	<p>Aktualizowanie baz danych i modułów aplikacji</p>
<p>ds.kaspersky.com</p> <p>Protokół: HTTPS</p> <p>Port: 443</p>	<p>Korzystanie z Kaspersky Security Network.</p>
<p>ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com</p> <p>Protokół: Dowolny</p> <p>Port: 443, 1443</p>	<p>Korzystanie z Kaspersky Security Network.</p>
<p>click.kaspersky.com redirect.kaspersky.com</p> <p>Protokół: HTTPS</p>	<p>Kliknij odnośniki w interfejsie</p>
<p>cr1.kaspersky.com</p>	<p>Infrastruktura kluczy publicznych (PKI)</p>

ocsp.kaspersky.com

Protokół: HTTP

Port: 80

Dodatek 6. Zdarzenia aplikacji w dzienniku zdarzeń systemu Windows

W dzienniku zdarzeń systemu Windows zapisywane są informacje o działaniu każdego modułu programu Kaspersky Endpoint Security, zdarzeniach szyfrowania danych, wykonaniu każdego zadania skanowania, zadania aktualizacji oraz zadania sprawdzania integralności, a także o ogólnym działaniu aplikacji.

[Audyt systemu](#) 


Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
201		Umowa licencja została naruszona.	✓
203		Licencja prawie utraciła ważność.	–
206		Nie odnaleziono baz danych lub są one uszkodzone.	–
207		Bazy danych są bardzo stare.	–
209		Automatyczne uruchamianie aplikacji jest wyłączone.	–
229		Błąd aktywacji.	✓
231		Wykryto aktywne zagrożenie. Zaawansowane leczenie musi zostać uruchomione.	–
2023		Serwery KSN są niedostępne.	–
237		Aplikacja uległa awarii podczas poprzedniej sesji.	✓
204		Licencja wkrótce utraci ważność.	–
208		Bazy danych są nieaktualne.	–
210		Automatyczna aktualizacja jest wyłączona.	–
211		Autoochrona jest wyłączona.	–
214		Składniki ochrony są wyłączone.	–
215		Komputer działa w trybie awaryjnym.	–
216		Istnieją nieprzetworzone pliki.	–
219		Zasada grupy została zastosowana.	✓
224		Aby zakończyć aktualizację, uruchom aplikację ponownie.	–
225		Wymagane jest ponowne uruchomienie komputera.	✓
226		Licencja uprawnia do korzystania ze składników, które nie są zainstalowane.	–
232		Uruchomiono zaawansowane leczenie.	–
233		Zaawansowane leczenie zostało zakończone.	–
230		Nieprawidłowy zapasowy kod aktywacyjny.	–
336		Nie można przywrócić obiektu z Kopii zapasowej.	✓
2001		Wykryto podejrzaną aktywność sieciową.	–
250		Przerwano zaszyfrowane połączenie.	✓
2021		Uczestnictwo w KSN jest wyłączone.	–
245		Przetwarzanie pewnych funkcji systemu operacyjnego jest wyłączone.	✓
235		Aplikacja uruchomiona.	✓
236		Aplikacja zatrzymana.	✓
213		Operacja dotycząca zasobów aplikacji została zablokowana przez Autoochronę.	–

217		Raport został wyczyszczony.	✓
220		Zasada grupy została wyłączona.	–
218		Ustawienia aplikacji zostały zmienione.	✓
227		Wszystkie składniki aplikacji określone w tej licencji zostały zainstalowane i działają w normalnym trybie.	–
238		Ustawienia subskrypcji uległy zmianie.	✓
239		Subskrypcja została odnowiona.	✓
335		Obiekt został przywrócony z Kopii zapasowej.	✓
2000		Wprowadź nazwę użytkownika i hasło.	–
2020		Uczestnictwo w KSN jest włączone.	–
2022		Serwery KSN są dostępne.	–
2024		Aplikacja działa i przetwarza dane zgodnie z odpowiednimi przepisami i korzysta z odpowiedniej infrastruktury.	✓
212		Zadanie nie może zostać uruchomione.	–
221		Zadanie zostało uruchomione.	–
222		Zadanie zostało zatrzymane.	–
223		Zadanie zostało zakończone.	–
227		Zainstalowane komponenty odpowiadają licencji.	–
240		Licencja wkrótce utraci ważność.	✓
708		Ustawienia zadania zostały pomyślnie zastosowane.	–










Wykrywanie zachowań

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
302		Wykryto szkodliwy obiekt.	–
313		Nie może zostać usunięty.	–
452		Działanie procesu zostało zakończone.	–
453		Nie można zakończyć procesu.	–
455		Zakończono wycofywanie.	–
331		Zablokowane.	–
307		Obiekt został usunięty.	–
323		Obiekt zostanie usunięty po ponownym uruchomieniu.	–
311		Nie można utworzyć kopii zapasowej.	–
303		Wykryto legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera lub prywatnych danych.	–
457		Przywrócono plik.	–
308		Utworzono kopię zapasową obiektu.	–
458		Przywrócono wartość rejestru.	–
459		Usunięto wartość rejestru.	–
329		Zmieniono nazwę obiektu.	–

[Ochrona przed exploitami](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
302		Wykryto szkodliwy obiekt.	–
331		Zablokowane.	–
455		Zakończono wycofywanie.	–
307		Obiekt został usunięty.	–
323		Obiekt zostanie usunięty po ponownym uruchomieniu.	–
457		Przywrócono plik.	–
458		Przywrócono wartość rejestru.	–
459		Usunięto wartość rejestru.	–
329		Zmieniono nazwę obiektu.	–

[Ochrona przed włamaniami](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
302		Wykryto szkodliwy obiekt.	–
312		Leczenie nie jest możliwe.	–
313		Nie może zostać usunięty.	–
317		Błąd przetwarzania.	✓
452		Działanie procesu zostało zakończone.	–
453		Nie można zakończyć procesu.	–
310		Nie można utworzyć kopii zapasowej.	–
314		Obiekt nie został przetworzony.	–
320		Obiekt zaszyfrowany.	–
321		Obiekt uszkodzony.	–
323		Obiekt zostanie usunięty po ponownym uruchomieniu.	–
324		Obiekt zostanie wyleczony po ponownym uruchomieniu.	–
303		Wykryto legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera lub prywatnych danych.	–
336		Nie można przywrócić obiektu z Kopii zapasowej.	✓
307		Obiekt został usunięty.	–
306		Obiekt został wyleczony.	–
301		Obiekt został przetworzony.	–
308		Utworzono kopię zapasową obiektu.	–
315		Obiekt został pominięty.	–
318		Wykryto archiwum.	–
319		Wykryto obiekt spakowany.	–
327		Nadpisany przy użyciu wcześniej wyleczonej kopii.	–
332		Informacje o wykrytym obiekcie.	–
322		Wykryto archiwum zabezpieczone hasłem.	–
335		Obiekt został przywrócony z Kopii zapasowej.	–
401		Aplikacja została umieszczona w grupie zaufanych.	–
402		Aplikacja została umieszczona w grupie z ograniczeniami.	–
403		Ochrona przed włamaniami została wywołana.	–
340		Obiekt znajduje się na liście zezwolonych Prywatnej sieci KSN.	✓

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
302		Wykryto szkodliwy obiekt.	✓
312		Leczenie nie jest możliwe.	–
313		Nie może zostać usunięty.	–
317		Błąd przetwarzania.	✓
452		Działanie procesu zostało zakończone.	–
453		Nie można zakończyć procesu.	–
310		Nie można utworzyć kopii zapasowej.	–
314		Obiekt nie został przetworzony.	–
320		Obiekt zaszyfrowany.	–
321		Obiekt uszkodzony.	–
323		Obiekt zostanie usunięty po ponownym uruchomieniu.	–
324		Obiekt zostanie wyleczony po ponownym uruchomieniu.	–
303		Wykryto legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera lub prywatnych danych.	–
336		Nie można przywrócić obiektu z Kopii zapasowej.	✓
307		Obiekt został usunięty.	–
306		Obiekt został wyleczony.	–
455		Zakończono wycofywanie.	–
301		Obiekt został przetworzony.	–
308		Utworzono kopię zapasową obiektu.	–
315		Obiekt został pominięty.	–
318		Wykryto archiwum.	–
319		Wykryto obiekt spakowany.	–
325		Nadpisany przy użyciu wcześniejszej wyleczonej kopii.	–
322		Wykryto archiwum zabezpieczone hasłem.	–
332		Informacje o wykrytym obiekcie.	–
335		Obiekt został przywrócony z Kopii zapasowej.	–
329		Zmieniono nazwę obiektu.	–
340		Obiekt znajduje się na liście zezwolonych Prywatnej sieci KSN.	✓

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
302		Wykryto szkodliwy obiekt.	✓
362		Zablokowano niebezpieczny odnośnik.	✓
363		Otwarto szkodliwy odnośnik.	✓
1201		Wykryto wcześniej otwarty niebezpieczny odnośnik.	✓
317		Błąd przetwarzania.	✓
303		Wykryto legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera lub prywatnych danych.	–
331		Zablokowane	–
341		Pobranie obiektu zostało zablokowane.	–
321		Obiekt uszkodzony.	–
301		Obiekt został przetworzony.	–
301		Odnośnik przetworzony.	–
332		Informacje o wykrytym obiekcie.	–
319		Wykryto obiekt spakowany.	–
318		Wykryto archiwum.	–
322		Wykryto archiwum zabezpieczone hasłem.	–
329		Zmieniono nazwę obiektu.	–
1211		Wykryto wcześniej otwarty szkodliwy odnośnik.	✓
370		Odnośnik znajduje się na liście zezwolonych Prywatnej sieci KSN.	✓
370		Obiekt znajduje się na liście zezwolonych Prywatnej sieci KSN.	✓

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
302		Wykryto szkodliwy obiekt.	✓
312		Leczenie nie jest możliwe.	–
317		Błąd przetwarzania.	✓
314		Obiekt nie został przetworzony.	–
303		Wykryto legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera.	–
321		Obiekt uszkodzony.	–
336		Nie można przywrócić obiektu z Kopii zapasowej.	–
307		Obiekt został usunięty.	–
306		Obiekt został wyleczony.	–
301		Obiekt został przetworzony.	–
308		Utworzono kopię zapasową obiektu.	–
318		Wykryto archiwum.	–
319		Wykryto obiekt spakowany.	–
329		Zmieniono nazwę obiektu.	–
332		Informacje o wykrytym obiekcie.	–
322		Wykryto archiwum zabezpieczone hasłem.	–
335		Obiekt został przywrócony z Kopii zapasowej.	–
340		Obiekt znajduje się na liście zezwolonych Prywatnej sieci KSN.	✓


[Zapora sieciowa](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
602		Aktywność sieciowa jest zablokowana.	–
601		Aktywność sieciowa jest dozwolona.	–

[Ochrona sieci](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
651		Wykryto atak sieciowy.	–

[Ochrona przed atakami BadUSB](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
2051		Klawiatura nie została zautoryzowana.	✓
2052		Błąd autoryzacji klawiatury.	✓
2050		Klawiatura zautoryzowana.	–








[Ochrona AMSI](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
302		Wykryto szkodliwy obiekt.	✓
2200		Zablokowano żądanie AMSI.	✓
317		Błąd przetwarzania.	✓
314		Obiekt nie został przetworzony.	–
320		Obiekt zaszyfrowany.	–
321		Obiekt uszkodzony.	–
303		Wykryto legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera lub prywatnych danych.	–
1512		Wynik skanowania obiektu został wysłany do zewnętrznej aplikacji.	–
301		Obiekt został przetworzony.	–
315		Obiekt został pominięty.	–
318		Wykryto archiwum.	–
319		Wykryto obiekt spakowany.	–
322		Wykryto archiwum zabezpieczone hasłem.	–
332		Informacje o wykrytym obiekcie.	–
340		Obiekt znajduje się na liście zezwolonych Prywatnej sieci KSN.	✓
329		Zmieniono nazwę obiektu.	–







[Kontrola aplikacji](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
702		Zabroniono uruchomienia aplikacji.	–
710		Zabroniony proces został uruchomiony przed Kaspersky Endpoint Security for Windows.	–
707		Błąd w ustawieniach zadania. Ustawienia zadania nie zostały zastosowane.	–
708		Ustawienia zadania zostały pomyślnie zastosowane.	–
701		Zezwolono na uruchomienie aplikacji.	–
703		Zabroniono uruchomienia aplikacji w trybie testowym.	–
704		Zezwolono na uruchomienie aplikacji w trybie testowym.	–






[Kontrola urządzeń](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
802		Działania na urządzeniu zostały zabronione.	–
809		Połączenie sieciowe zablokowane.	–
803		Tymczasowy dostęp do urządzenia został aktywowany.	
801		Działania na urządzeniu zostały dozwolone.	–
808		Operacja na pliku została wykonana.	–




[Kontrola sieci](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
752		Dostęp zabroniony.	–
753		Ostrzeżenie o niechcianej zawartości.	–
754		Uzyskano dostęp do niechcianej zawartości po wyświetleniu ostrzeżenia.	–
751		Dostęp dozwolony.	–
751		Otwarto dozwoloną stronę.	–

[Adaptacyjna kontrola anomalii](#)
















Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
2200		Zablokowano akcję procesu.	
2201		Pominięto akcję procesu.	–

[Szyfrowanie danych](#) 

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
904		Błąd podczas stosowania reguł szyfrowania/odszyfrowywania pliku.	✓
912		Błąd podczas szyfrowania/odszyfrowywania pliku.	✓
940		Zablokowano dostęp do pliku.	✓
951		Błąd podczas włączania trybu przenośnego.	✓
953		Błąd podczas wyłączenia trybu przenośnego.	✓
931		Błąd podczas tworzenia zaszyfrowanego pakietu.	✓
1305		Błąd podczas szyfrowania/odszyfrowywania urządzenia.	✓
1311		Nie powiodło się załadowanie modułu szyfrowania.	✓
1340		Zadanie zarządzające kontami Agenta autoryzacji zostało zakończone z błędem.	✓
1312		Zasada nie może zostać zastosowana.	✓
1342		Aktualizacja FDE zakończyła się niepowodzeniem.	✓
1344		Wycofanie aktualizacji Szyfrowania całego dysku zakończyło się błędem.	✓
903		Przerwano stosowanie reguł szyfrowania/odszyfrowywania pliku.	–
914		Przerwano szyfrowanie/odszyfrowywanie pliku.	–
1303		Przerwano szyfrowanie/odszyfrowywanie urządzenia.	–
1306		Użytkownik zrezygnował z zasady szyfrowania.	–
1345		Nie udało się zainstalować lub zaktualizować sterowników Kaspersky Disk Encryption w obrazie WinRE.	✓
901		Uruchomiono stosowanie reguł szyfrowania/odszyfrowywania pliku.	–
902		Zakończono stosowanie reguł szyfrowania/odszyfrowywania pliku.	–
905		Wznowiono stosowanie reguł szyfrowania/odszyfrowywania pliku.	–
910		Uruchomiono szyfrowanie/odszyfrowywanie pliku.	–
911		Zakończono szyfrowanie/odszyfrowywanie pliku.	–
913		Plik nie został zaszyfrowany, ponieważ jest wykluczony.	–
950		Włączono tryb przenośny.	–
952		Wyłączono tryb przenośny.	–
1301		Uruchomiono szyfrowanie/odszyfrowywanie urządzenia.	–
1302		Zakończono szyfrowanie/odszyfrowywanie urządzenia.	–
1304		Wznowiono szyfrowanie/odszyfrowywanie urządzenia.	–
1310		Wczytano moduł szyfrujący.	–
1307		Urządzenie nie jest zaszyfrowane.	–
1308		Proces szyfrowania/odszyfrowywania urządzenia został przełączony do trybu aktywnego.	–

1309		Proces szyfrowania/odszyfrowywania urządzenia został przełączony do trybu pasywnego.	–
1330		Utworzono nowe konto Agenta autoryzacji.	–
1331		Usunięto konto Agenta autoryzacji.	–
1332		Zmieniono hasło do konta Agenta autoryzacji.	–
1333		Pomyślne logowanie Agenta autoryzacji.	–
1334		Nieudana próba logowania Agenta autoryzacji.	–
1335		Dostęp do dysku twardego uzyskany przy użyciu procedury dostępu do zaszyfrowanych urządzeń.	–
1336		Próba dostępu do dysku twardego przy użyciu procedury dostępu do zaszyfrowanych urządzeń nie powiodła się.	–
1337		Konto nie zostało dodane. To konto już istnieje.	–
1338		Konto nie zostało zmodyfikowane. To konto nie istnieje.	–
1339		Konto nie zostało usunięte. To konto nie istnieje.	–
1341		Aktualizacja FDE zakończyła się powodzeniem.	✓
1343		Cofanie aktualizacji FDE zakończyło się powodzeniem.	✓
1346		Nie udało się odinstalować sterowników Kaspersky Disk Encryption w obrazie WinRE.	✓
1370		Klucz odzyskiwania funkcji BitLocker został zmieniony.	✓

Endpoint Sensor

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
2100		Serwer Kaspersky Anti Targeted Attack Platform jest niedostępny.	–
2105		Uruchomienie aplikacji zostało zablokowane.	✓
2106		Otwarcie dokumentu zostało zablokowane.	✓
2112		Wszystkie procesy uruchomione z pliku obrazu lub strumienia zostały zakończone.	✓
2113		Uruchamianie aplikacji.	✓
2111		Plik lub strumień został usunięty przez administratora serwera Kaspersky Anti Targeted Attack Platform.	✓
2110		Plik został przywrócony z kwarantanny z serwera Kaspersky Anti Targeted Attack Platform przez administratora.	✓
2109		Plik został przeniesiony do kwarantanny na serwer Kaspersky Anti Targeted Attack Platform przez administratora.	✓
2107		Aktywność sieciowa aplikacji firm trzecich została zablokowana.	✓
2108		Aktywność sieciowa aplikacji firm trzecich została odblokowana.	✓
2104		Zadania z serwera Kaspersky Anti Targeted Attack Platform są przetwarzane.	–
2103		Przetwarzanie zadań z serwera Kaspersky Anti Targeted Attack Platform jest nieaktywne.	–
2101		Składnik Endpoint Sensor nawiązał połączenie z serwerem.	–
2102		Połączenie z serwerem Kaspersky Anti Targeted Attack Platform zostało przywrócone.	–


[Skanowanie komputera](#)

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
302		Wykryto szkodliwy obiekt.	✓
312		Leczenie nie jest możliwe.	–
313		Nie może zostać usunięty.	–
317		Błąd przetwarzania.	–
452		Działanie procesu zostało zakończone.	–
453		Nie można zakończyć procesu.	–
310		Nie można utworzyć kopii zapasowej.	–
314		Obiekt nie został przetworzony.	–
320		Obiekt zaszyfrowany.	–
321		Obiekt uszkodzony.	–
323		Obiekt zostanie usunięty po ponownym uruchomieniu.	–
324		Obiekt zostanie wyleczony po ponownym uruchomieniu.	–
303		Wykryto legalne oprogramowanie, które może zostać wykorzystane przez przestępców do uszkodzenia komputera lub prywatnych danych.	–
336		Nie można przywrócić obiektu z Kopii zapasowej.	✓
307		Obiekt został usunięty.	–
306		Obiekt został wyleczony.	–
455		Zakończono wycofywanie.	–
301		Obiekt został przetworzony.	–
308		Utworzono kopię zapasową obiektu.	–
315		Obiekt został pominięty.	–
318		Wykryto archiwum.	–
319		Wykryto obiekt spakowany.	–
327		Nadpisany przy użyciu wcześniejszej wyleczonej kopii.	–
332		Informacje o wykrytym obiekcie.	–
322		Wykryto archiwum zabezpieczone hasłem.	–
335		Obiekt został przywrócony z Kopii zapasowej.	✓
329		Zmieniono nazwę obiektu.	–
340		Obiekt znajduje się na liście zezwolonych Prywatnej sieci KSN.	✓

[Sprawdzanie integralności](#) 

Kody zdarzeń




ID zdarzenia		Opis	Włączono domyślnie
2002		Sprawdzanie sygnatury modułu systemu zakończyło się niepowodzeniem	-

[Aktualizacja baz danych](#) 

Kody zdarzeń

ID zdarzenia		Opis	Włączono domyślnie
1011		Błąd podczas aktualizacji składnika.	–
1012		Błąd podczas dystrybucji aktualizacji składników.	–
1014		Lokalny błąd aktualizacji.	–
1015		Sieciowy błąd aktualizacji.	–
1017		Nie można uruchomić dwóch zadań w tym samym czasie.	–
1018		Błąd podczas weryfikacji baz danych oraz modułów aplikacji.	–
1019		Błąd współdziałania z Kaspersky Security Center.	–
1021		Nie wszystkie składniki zostały uaktualnione.	–
1023		Aktualizacja została pomyślnie zakończona, dystrybucja uaktualnień nie powiodła się.	–
101		Wystąpił błąd wewnętrzny.	✓
2153		Instalacja poprawki nie powiodła się.	–
2156		Wycofanie poprawki nie powiodło się.	–
1016		Operacja została anulowana przez użytkownika.	–
1001		Wybrano źródło uaktualnień.	–
1002		Wybrano serwer proxy.	–
1003		Pobieranie pliku.	–
1004		Plik został pobrany.	–
1005		Plik został zainstalowany.	–
1006		Plik został uaktualniony.	–
1007		Plik został przywrócony z powodu błędu aktualizacji.	–
1008		Aktualizacja plików.	–
1009		Dystrybucja uaktualnień.	–
1010		Wycofywanie plików.	–
1013		Tworzenie listy plików do pobrania.	–
1020		Brak dostępnych aktualizacji.	–
1022		Zadanie dystrybucji uaktualnień zostało pomyślnie zakończone.	–
2150		Pobieranie poprawek.	–
2151		Instalowanie poprawek.	–
2152		Poprawka zainstalowana.	–
2154		Wycofywanie poprawki.	–
2155		Poprawka wycofana.	–



Kody zdarzeń



ID zdarzenia		Opis	Włączono domyślnie
2252		Nie może zostać usunięty.	–
2253		Statystyki zadania czyszczenia.	–
2251		Obiekt został usunięty.	–



Dodatek 7. Zdarzenia aplikacji w dzienniku zdarzeń Kaspersky Security Center

W dzienniku zdarzeń Kaspersky Security Center zapisywane są informacje o działaniu każdego modułu programu Kaspersky Endpoint Security, zdarzeniach szyfrowania danych, wykonaniu każdego zadania skanowania, zadania aktualizacji oraz zadania sprawdzania integralności, a także o ogólnym działaniu aplikacji.







Zdarzenia Kaspersky Endpoint Security for Windows


ID zdarzenia		Opis	Ustawienia
GNRL_EV_VIRUS_FOUND		Wykryto szkodliwy obiekt.	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 to suma kontrol obiektu (SHA256). GNRL_EA_PARAM_2 to nazwa obiekt GNRL_EA_PARAM_5 to nazwa obiekt zgodnie z klasyfikacją Kaspersky. GNRL_EA_PARAM_7 to nazwa użytkownika sesji. GNRL_EA_PARAM_8 to typ zagrożenia przykład, Trojware. GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez prywatną KSN (denylist): true lub false. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
GNRL_EV_SUSPICIOUS_OBJECT_FOUND		Wykryto legalne oprogramowanie, które może zostać wykorzystane	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 to suma kontrol obiektu (SHA256). GNRL_EA_PARAM_2 to nazwa obiekt

		przez przestępców do uszkodzenia komputera lub prywatnych danych	<ul style="list-style-type: none"> GNRL_EA_PARAM_5 to nazwa zagrożenia na przykład, EICAR-Test-File. GNRL_EA_PARAM_7 to nazwa użytkownika sesji. GNRL_EA_PARAM_8 to typ zagrożenia na przykład, Trojware.
GNRL_EV_OBJECT_CURED		Obiekt został wyleczony.	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 to suma kontrolna obiektu (SHA256). GNRL_EA_PARAM_2 to nazwa obiektu GNRL_EA_PARAM_3 to data utworzenia obiektu (opcjonalne). GNRL_EA_PARAM_5 to nazwa obiektu zgodnie z klasyfikacją Kaspersky. GNRL_EA_PARAM_7 to nazwa użytkownika sesji. GNRL_EA_PARAM_8 to typ zagrożenia na przykład, Trojware. GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez prywatną KSN (denylist): true lub false. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
GNRL_EV_OBJECT_DELETED		Obiekt został usunięty.	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 to suma kontrolna obiektu (SHA256). GNRL_EA_PARAM_2 to nazwa obiektu GNRL_EA_PARAM_3 to data utworzenia obiektu (opcjonalne). GNRL_EA_PARAM_5 to nazwa obiektu zgodnie z klasyfikacją Kaspersky. GNRL_EA_PARAM_7 to nazwa użytkownika sesji. GNRL_EA_PARAM_8 to typ zagrożenia na przykład, Trojware.

			<ul style="list-style-type: none"> GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez prywatną KSN (denylist): true lub false. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
GNRL_EV_OBJECT_NOTCURED		Leczenie nie jest możliwe.	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 to suma kontrol obiektu (SHA256). GNRL_EA_PARAM_2 to nazwa obiekt GNRL_EA_PARAM_3 to data utworze obiektu (opcjonalne). GNRL_EA_PARAM_5 to nazwa obiekt zgodnie z klasyfikacją Kaspersky. GNRL_EA_PARAM_7 to nazwa użytkc sesji. GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez prywatną KSN (denylist): true lub false. Wersja EDR. Identyfikator zagrożenia w EDR. Suma kontrolna MD5 obiektu.
GNRL_EV_PASSWD_ARCHIVE_FOUND		Wykryto archiwum zabezpieczone hasłem.	<ul style="list-style-type: none"> GNRL_EA_PARAM_2 to nazwa obiekt GNRL_EA_PARAM_3 to data utworze obiektu (opcjonalne). GNRL_EA_PARAM_7 to nazwa użytkc sesji. GNRL_EA_PARAM_9 to dodatkowe informacje o wykrytym obiekcie: Składnik aplikacji (engine). Technologia wykrywania zagrożeń (method). Zagrożenie wykryte przez prywatną KSN (denylist): true lub false.
GNRL_EV_ATTACK_DETECTED		Wykryto atak sieciowy (Ochrona sieci).	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 to nazwa ataku.

			<ul style="list-style-type: none"> • GNRL_EA_PARAM_8 to suma kontrol obiektu (SHA256). • GNRL_EA_PARAM_9 to wersja aplikacji którą użytkownik próbuje uruchomić
GNRL_EV_APP_LAUNCH_TESTED_DENIED		Zabroniono uruchomienia aplikacji w trybie testowym (Kontrola aplikacji).	<ul style="list-style-type: none"> • GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_3 to ręcznie utworzony identyfikator kategorii. • GNRL_EA_PARAM_4 to identyfikator zabezpieczeń konta (SID). • GNRL_EA_PARAM_5 to informacje o cyfrowym podpisie aplikacji. • GNRL_EA_PARAM_6 to nazwa pliku wykonywalnego aplikacji (na przykład chrome.exe). • GNRL_EA_PARAM_7 to ścieżka do pliku wykonywalnego. • GNRL_EA_PARAM_8 to suma kontrol obiektu (SHA256). • GNRL_EA_PARAM_9 to wersja aplikacji którą użytkownik próbuje uruchomić
GNRL_EV_APP_LAUNCH_TESTED_ALLOW		Zezwolono na uruchomienie aplikacji w trybie testowym (Kontrola aplikacji).	<ul style="list-style-type: none"> • GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_3 to ręcznie utworzony identyfikator kategorii. • GNRL_EA_PARAM_4 to identyfikator zabezpieczeń konta (SID). • GNRL_EA_PARAM_5 to identyfikator kategorii aplikacji (opcjonalnie).
GNRL_EV_AC_USER_REQUEST		Wiadomość do administratora dotycząca zablokowania uruchomienia aplikacji (Kontrola aplikacji).	<ul style="list-style-type: none"> • c_er_descr to wiadomość do użytkownika. • GNRL_EA_PARAM_2 to nazwa użytkownika sesji. • GNRL_EA_PARAM_6 to nazwa pliku wykonywalnego aplikacji (na przykład chrome.exe).

			<ul style="list-style-type: none"> • GNRL_EA_PARAM_7 to ścieżka do pl wykonywalnego. • GNRL_EA_PARAM_8 to suma kontrol obiektu (SHA256). • GNRL_EA_PARAM_9 to wersja aplikacji którą użytkownik próbuje uruchomić
GNRL_EV_WEB_URL_BLOCKED		Dostęp zabroniony (Kontrola sieci).	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 to adres interne • GNRL_EA_PARAM_2 to nazwa użytkc sesji. • GNRL_EA_PARAM_3 to nazwa reguły Kontroli sieci.
GNRL_EV_WEB_URL_WARNING		Ostrzeżenie o niechcianej zawartości (Kontrola sieci).	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 to adres interne • GNRL_EA_PARAM_2 to nazwa użytkc sesji. • GNRL_EA_PARAM_3 to nazwa reguły Kontroli sieci.
GNRL_EV_WC_USER_REQUEST		Wiadomość do administratora dotycząca zablokowania dostępu do strony internetowej (Kontrola sieci).	<ul style="list-style-type: none"> • c_er_descr to wiadomość do użytkownika. • GNRL_EA_PARAM_1 to adres interne • GNRL_EA_PARAM_2 to nazwa użytkc sesji.
GNRL_EV_DC_USER_REQUEST		Wiadomość do administratora dotycząca zablokowania dostępu do urządzenia (Kontrola urządzeń).	<ul style="list-style-type: none"> • c_er_descr to wiadomość do użytkownika. • GNRL_EA_PARAM_1 to ID sprzętu (H • GNRL_EA_PARAM_2 to nazwa użytkc sesji.
GNRL_EV_DEVCTRL_DEV_PLUGGED		Podłączone urządzenie (Kontrola urządzeń).	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 to ID sprzętu (H • GNRL_EA_PARAM_2 to nazwa użytkc sesji.
GNRL_EV_DEVCTRL_DEV_UNPLUGGED		Odłączone urządzenie (Kontrola urządzeń).	<ul style="list-style-type: none"> • GNRL_EA_PARAM_1 to ID sprzętu (H • GNRL_EA_PARAM_2 to nazwa użytkc sesji.

GNRL_EV_DEVCTRL_DEV_PLUG_DENIED		Zablokowano podłączone urządzenie (Kontrola urządzeń).	<ul style="list-style-type: none"> GNRL_EA_PARAM_1 to ID sprzętu (H GNRL_EA_PARAM_2 to nazwa użytkownika sesji.
---------------------------------	---	--	---

Dodatek 8. Obsługiwane rozszerzenia plików dla Zapobiegania wykonywaniu

Kaspersky Endpoint Security obsługuje zapobieganie otwierania plików formatu office w pewnych aplikacjach. Informacje o obsługiwanych rozszerzeniach plików i aplikacji znajdują się w następującej tabeli.

Obsługiwane rozszerzenia plików dla Zapobiegania wykonywaniu

Nazwa aplikacji	Plik wykonywalny	Rozszerzenie pliku
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltn xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm

		ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

Dodatek 9. Obsługiwane interpretory skryptów

Zapobieganie wykonywaniu obsługuje następujące interpretory skryptów:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe

- msixexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacyelevated.exe
- wscript.exe
- wwaahost.exe

Zapobieganie wykonywaniu obsługuje pracę z aplikacjami Java w środowisku uruchomieniowym Java (procesy java.exe i javaw.exe).

Dodatek 10. Obszar skanowania IOC w rejestrze (RegistryItem)

Jeśli dodasz typ danych RegistryItem do obszaru skanowania IOC, Kaspersky Endpoint Security skanuje następujące klucze rejestru:

HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Dodatek 11. Wymagania pliku IOC

Podczas tworzenia zadań Skanowanie IOC rozważ następujące ograniczenia i wymagania [pliku IOC](#):

- Kaspersky Endpoint Detection and Response Optimum obsługuje pliki IOC z rozszerzeniami IOC i XML w otwartym standardzie OpenIOC w wersjach 1.0 i 1.1 dla opisanego wskaźników naruszeń bezpieczeństwa.
- Jeśli podczas tworzenia zadania Skanowanie IOC przesłałeś pliki IOC, z których niektóre nie są obsługiwane, gdy zadanie jest uruchomione, aplikacja używa tylko obsługiwanych plików IOC.
- Jeśli podczas tworzenia zadania Skanowanie IOC przesyłasz tylko nieobsługiwane pliki IOC, zadanie może wciąż być uruchomione, ale nie zostaną wykryte żadne wskaźniki naruszeń bezpieczeństwa.
- Błędy semantyczne i nieobsługiwane warunki IOC i znaczniki w plikach IOC nie powodują błędów wykonania zadania. W takich sekcjach plików IOC aplikacja nie wykrywa dopasowania.

- [Identyfikatory wszystkich plików IOC](#) używane w pojedynczym zadaniu Skanowanie IOC muszą być unikatowe. Jeśli istnieją pliki IOC z takim samym identyfikatorem, mogą wpłynąć na wyniki wykonania zadania.
- Rozmiar pojedynczego pliku IOC nie może przekraczać 3 MB. Używanie większych plików spowoduje zakończenie zadania Skanowanie IOC z błędem. Całkowity rozmiar wszystkich plików dodanych do zbioru IOC może przekroczyć 3 MB.
- Zalecane jest utworzenie jednego pliku IOC na zagrożenie. To ułatwia analizowanie wyników zadania Skanowanie IOC.

Plik, który możesz pobrać, klikając poniższy odnośnik, zawiera tabelę z pełną listą warunków IOC standardu OpenIOC, który jest obsługiwany przez rozwiązanie Kaspersky Endpoint Detection and Response.

 [POBIERZ PLIK IOC TERMS.XLSX](#)

Funkcje i ograniczenia obsługi aplikacji dla standardu OpenIOC są wyświetlone w poniższej tabeli.

Funkcje i ograniczenia obsługi OpenIOC w wersji 1.0 i 1.1.

Obsługiwane warunki	OpenIOC 1.0: is isnot (jako wyjątek z zestawu) contains containsnot (jako wyjątek z zestawu) OpenIOC 1.1: is contains starts-with ends-with matches greater-than less-than
Obsługiwane atrybuty warunku	OpenIOC 1.1: preserve-case negate
Obsługiwane operatory	ORAZ LUB
Obsługiwane typy danych	"date": data (stosowane warunki: is, greater-than, less-than) "int": liczba całkowita (stosowane warunki: is, greater-than, less-than) "string": ciąg znaków (stosowane warunki: is, contains, matches, starts-with, ends-with) "duration": czas trwania w sekundach (stosowane warunki: is, greater-than, less-than)
Funkcje interpretacji typu danych	Typy danych "boolean string", "restricted string", "md5", "IP", "sha256" i "base64Binary" są interpretowane jako ciąg znaków. Aplikacja obsługuje interpretację ustawienia Zawartość dla typów danych int i date, gdy jest ona ustawiona w postaci przedziałów czasu:

OpenIOC 1.0:

Przy użyciu operatora D0 w polu Zawartość:

```
<Content type="int">49600 TO 50700</Content>
```

```
<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>
```

```
<Content type="int">[154192 TO 154192]</Content>
```

OpenIOC 1.1:

Przy użyciu warunków `greater-than` i `less-than`

Przy użyciu operatora D0 w polu Zawartość

Aplikacja obsługuje interpretację typów danych `date` i `duration`, jeśli wskaźniki są ustawione w formacie ISO 8601, Zulu Time Zone, UTC.

Informacje o kodzie firm trzecich

Informacje o kodzie firm trzecich znajdują się w pliku legal_notices.txt przechowywanym w folderze instalacyjnym aplikacji.

Informacje o znakach towarowych

Zastrzeżone znaki towarowe i usługowe stanowią odpowiednio własność ich właścicieli.

Adobe, Acrobat, Flash, Reader i Shockwave są zastrzeżonymi znakami towarowymi lub znakami towarowymi Adobe Systems Incorporated zarejestrowanymi w Stanach Zjednoczonych i/lub innych krajach.

Apple, FireWire, iTunes i Safari są znakami towarowymi firmy Apple Inc., zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

AutoCAD jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Autodesk, Inc. i/lub jej oddziałów w Stanach Zjednoczonych i/lub innych krajach.

Słowo, znak i logo Bluetooth są własnością firmy Bluetooth SIG, Inc.

Borland jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Borland Software Corporation.

Android i Google Chrome są znakami towarowymi firmy Google, Inc.

Citrix i Citrix Provisioning Services oraz XenDesktop są znakami towarowymi Citrix Systems, Inc. i/lub jednego lub więcej oddziałów i mogą być zarejestrowane w Urzędzie Patentowym w Stanach Zjednoczonych i innych krajach.

Dell to znak towarowy firmy Dell, Inc. lub jej oddziałów.

dBase jest znakiem towarowym firmy dataBased Intelligence, Inc.

EMC to znak towarowy lub zastrzeżony znak towarowy EMC Corporation, zarejestrowany w Stanach Zjednoczonych i innych krajach.

Radmin jest zarejestrowanym znakiem towarowym firmy Famatech.

IBM jest znakiem towarowym firmy International Business Machines Corporation, zarejestrowanym w wielu jurysdykcjach na świecie.

ICQ jest znakiem towarowym i/lub znakiem usługowym firmy ICQ LLC.

Intel jest znakiem towarowym firmy Intel Corporation w Stanach Zjednoczonych i/lub innych krajach.

IOS jest zastrzeżonym znakiem towarowym firmy Cisco Systems, Inc. i/lub jej oddziałów na terenie Stanów Zjednoczonych i innych krajów.

Lenovo i ThinkPad są znakami towarowymi firmy Lenovo, zarejestrowanymi w Stanach Zjednoczonych i/lub innych krajach.

Linux jest zastrzeżonym znakiem towarowym firmy Linus Torvalds w Stanach Zjednoczonych i innych krajach.

Logitech jest zastrzeżonym znakiem towarowym lub znakiem towarowym firmy Logitech w Stanach Zjednoczonych i/lub innych krajach.

LogMeIn Pro i Remotely Anywhere to znaki towarowe firmy LogMeIn, Inc.

Mail.ru jest zastrzeżonym znakiem towarowym firmy Mail.Ru, LLC.

McAfee to znak towarowy lub zastrzeżony znak towarowy firmy McAfee, Inc., zarejestrowany w Stanach Zjednoczonych i innych krajach.

Microsoft, Access, Active Directory, ActiveSync, BitLocker, Excel, Internet Explorer, LifeCam Cinema, MSDN, MultiPoint, Outlook, PowerPoint, PowerShell, Visual Basic, Visual FoxPro, Windows, Windows PowerShell, Windows Server, Windows Store, MS-DOS, Surface i Hyper-V są zastrzeżonymi znakami towarowymi firmy Microsoft Corporation, zarejestrowanymi w Stanach Zjednoczonych i innych krajach.

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

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

VERISIGN jest zastrzeżonym lub niezastrzeżonym znakiem towarowym firmy VeriSign, Inc. i jej oddziałów, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

VMware i VMware ESXi są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy VMware, Inc., zarejestrowanymi w Stanach Zjednoczonych i/lub innych jurysdykcjach.

Thawte jest znakiem towarowym lub zastrzeżonym znakiem towarowym firmy Symantec Corporation lub jej oddziałów, zarejestrowanym w Stanach Zjednoczonych i innych krajach.

SAMSUNG jest znakiem towarowym SAMSUNG, zarejestrowanym w Stanach Zjednoczonych i innych krajach.